Data privacy and protection in AI-driven healthcare

S Mahomed, BCom, LLB, LLM, PhD

Department of Jurisprudence, School of Law, University of South Africa, Pretoria, South Africa; admitted attorney of the High Court of South Africa

***Corresponding author**: S Mahomed (mahoms1@unisa.ac.za)*

The concept of keeping health data private is constantly being tested, as what constitutes health data has grown significantly, now including massive amounts of personal information from a variety of sources, such as genomic data, radiological images, medical records, and non-health data converted into health data. These numerous sources of data, collectively termed 'biomedical big data' (BD), comprise a health data ecosystem that has altered the landscape of health research. BD, which is often referred to as the 'new oil', provides a natural blueprint for artificial intelligence (AI) to thrive and to generate and advance knowledge exponentially. However, while the need for data grows, data breaches are on the rise, specifically in the healthcare sector. The rise in local data breaches underscores the urgent need to translate paper into practice by strengthening systems and enforcing the ethico-legal framework governing the processing of data in SA, including ways in which to efficiently handle its misuse. This involves ensuring the adoption of ethically sound practices, adaptable infrastructure, and robust governance that is specific to the SA context.

Keywords: artificial intelligence, healthcare, data breaches, privacy, governance

S Afr Med J 2025;115(5b):e3666. https://doi.org/10.7196/SAMJ.2025.v115i5b.3666

Data breaches are on the rise, specifically in the healthcare sector which accounted for 32% of all data breaches between 2015 and 2022. This figure is almost double the number recorded in the financial and manufacturing sectors.[1] Further statistics show that during the second quarter of 2023, the healthcare sector experienced an average of 1 744 attacks per week, reflecting a significant year-on-year increase of 30%. Notably, Africa experienced the highest average number of weekly cyber-attacks per organisation, with an average of 2 164 attacks,[2] which is a significant year-on-year increase of 23% compared with the same period in 2022. In addition, a 2023 briefing by the South African Council for Scientific and Industrial Research (CSIR) reported that SA was the eighth most targeted country worldwide for ransomware.[3] Not long after the CSIR released its report, SA news reported that all the internal and external information technology (IT) systems of the National Health Laboratory Service (NHLS) remained down, following an attempted ransomware attack by the BlackSuit hacking group who reportedly stole approximately 1.2 terabytes of data (equivalent to about 30 large moving boxes full of documents or the contents of 25 000 books), including third-party, client and patient information.[4] A few weeks after initial news of the NHLS cyber-attack broke in June 2024, it was reported that local mining giant Sibanye-Stillwater, one of the world's biggest producers of platinum and gold, suffered a cyber-attack. The attacks on the mining giant and the NHLS come after a slew of cybercriminal acts targeting high-profile entities in SA.[5]

The NHLS is considered the backbone of SA's health system, providing diagnostic tests and holding electronic records for patients using the public health system; it also offers some highly specialised tests that are not available in the private sector.[4] The consequences of this cyber-attack were that doctors were forced to revert to paper records, and there were delayed test results and operations, with patients being exposed to suffering and harm. It also disrupted financial and human resource systems, affecting the NHLS' ability to pay staff and suppliers. In addition to stealing data, the hacking group also erased large portions of data, including backups.[6] Apart from major disruptions to routine healthcare services countrywide, the cyberattack paused plans for paediatric tuberculosis tests. Fortunately, on 22 August 2024, approximately two months after news of the cyber-attack was reported, it was announced that all operations were restored at the NHLS.[7] However, the lasting effects of the cyber-attack have taken a toll on the NHLS, which is now looking to upgrade its cyber-defence mechanisms.

This article aims to address the connection between artificial intelligence (AI) and data for healthcare in South Africa while recognising that data and AI are fundamentally linked. It further identifies that the increased demand for data has highlighted systems vulnerabilities and sets out current legal protection in place to safeguard data. In addition, the article considers whether these protections are sufficient and translatable to our local context and offers certain recommendations towards improvement.

Can the use of data be controlled?

As AI systems require data to succeed, a question to consider is whether the use of such data can be sufficiently controlled. A few weeks prior to the news of the NHLS ransomware attack being announced, information was released that Informa, the parent company of academic publisher Taylor & Francis, signed a $10 million data-access agreement with Microsoft.[8] The AI partnership agreement provides Microsoft 'nonexclusive access to Advanced Learning Content' across Taylor & Francis's nearly 3 000 academic journals. After the initial access fee of $10 million, Informa said it would receive recurring payments for the next three years.[8] The agreement allows Microsoft to train its AI models on Taylor & Francis' extensive catalogue of scholarly publications. An immediate concern was not the fact that such a partnership agreement took place, but rather that authors were not informed about the bulk sale of their research, including how their research will be republished and cited by the publisher's AI tools. Informa's half-year results published during July 2024 confirmed a second major partnership with another AI company, and AI-related revenues are expected to exceed $75 million for the year. The data-access agreements, it said, 'are a source of significant new value for Taylor & Francis …'[8] However, whether academics

will financially benefit from the agreement is not clear, with some scholars coining the agreement as a 'money making data grab', questioning why academics were not provided with an opportunity to opt out of it.[8]

The examples of the attempted NHLS ransomware attack and the Informa - Microsoft data access agreement point to the fact that the more data required, coupled with more complex technology, the more we need to understand the vulnerability of our systems and have greater control over how our data are used. However, system vulnerabilities and data controls are constantly challenged by rapid developments in AI which require vast data sets as part of the design for AI initiatives, including in healthcare.

AI and data in healthcare

The concept of keeping health data private is constantly being tested, as what constitutes health data has grown significantly, now including massive amounts of personal information from a variety of sources, such as genomic data, radiological images, medical records, and non-health data converted into health data.[9] These numerous sources of data, collectively termed as 'biomedical big data', comprise a health data ecosystem that has altered the landscape of health research. This data ecosystem has both potential for innovation and substantial ethical challenges. The global push for interconnection, enabled by open science, open access and open data, has an impact on data sharing for research purposes. In the context of patient-centered care, it is critical to identify the ongoing expansion of data in terms of volume, variety and velocity, which is catalysing a transition towards Big Data (BD). To extract valuable insights from the extensive data generated by individual patients, it is necessary to validate, process and integrate these data into systems that can generate new value within healthcare organisations. The increasing impact of BD has encouraged healthcare organisations to adopt AI and cultivate the requisite skills to effectively utilise BD analytics (BDA).[9] AI pilot projects were deployed in Africa during the mid-1980s already, therefore the concept of AI in healthcare is not a completely new phenomenon. What is new, is the development of normative documents in recent years that comprise principles and guidance for ethical and socially responsible AI. However, it is prudent to note that the 'global consensus' regarding the development of normative documents to guide ethically and socially responsible uses of AI does not always incorporate the uniquely African perspective.[10] Although the application of AI in low- and middle-income countries (LMICs) may be limited, due to varying factors, digital health technologies are already widely used in LMICs for data collection, dissemination of health information by mobile phones and extended use of electronic medical records on open-software platforms and cloud computing (among others).[11] AI and BD are intrinsically linked, as AI systems heavily rely on data to function effectively, particularly in interpreting and deriving insights from vast datasets. A prime example of the synergy between AI and BD is the way researchers and healthcare professionals gained a better understanding of COVID-19.[12] By leveraging large datasets, including epidemiological data, clinical records and genomic sequences, AI algorithms were able to analyse patterns, identify risk factors and develop predictive models to assist during the pandemic. BD, which is often referred to as the 'new oil', provides a natural blueprint for AI to thrive and to generate and advance knowledge exponentially. Thus, a constant stream of data and the use of AI is ubiquitous in the research space. With regard to research, AI increases efficiency, productivity, innovation and collaboration.

A 2023 *Nature* survey of approximately 1 600 researchers worldwide revealed an overall positive sentiment regarding the increasing use of AI tools in scientific research. But, while more than half of the respondents anticipated AI tools to be 'very important' or 'essential' in their fields within the next decade, researchers also expressed concerns about how AI is transforming research, including issues related to bias, fraud and irreproducibility.[13] It is evident that BD is part of the design for AI initiatives in healthcare – opening new opportunities for data-driven discovery. However, they also raise ethical challenges, as we have seen in the case of the NHLS data breach. Nevertheless, just when we are beginning to grapple with issues around the ethical management of AI in healthcare, new developments such as Artificial General Intelligence and Artificial Superintelligence emerge. These are advanced AI systems that meet or exceed the skills of human experts.[14] Although theoretical for now, we need to prepare ourselves for AI programmes that can independently interpret data and perform reasoning tasks without human intervention at performance levels exceeding those of human experts. Accordingly, we need to consider that AI may become responsible for traditional clinical tasks such as diagnostics, data-driven decision-making, and elements of cognitive empathy, in which they may outperform humans. For example, a physician will diagnose and customise treatments based on clinical knowledge and familiarity with similar cases. Advanced AI can apply the same processes but with an added advantage to access medical knowledge far beyond that of any individual human, and an ability to link this knowledge with personalised patient data.[14] Thus, the capabilities of AI systems which depend on data to flourish, appear to be unlimited; however, we need to consider whether our legal safeguards offer sufficient protections.

Legal landscape

Presently, the right to privacy is a fundamental right protected under section 14 of the Constitution (1996). In addition to protections developed under this Constitution, the rights to confidentiality and privacy in the health context are further safeguarded in various laws and policy documents. The National Health Act 61 of 2003 (NHA) provides for the broad protection of patient privacy and confidentiality. The Protection of Personal Information Act 4 of 2013 (POPIA) – which derives guidance from section 14 of the Constitution – is the most significant piece of legislation to consider where the processing of personal information is concerned. Section 1 of POPIA defines personal information broadly and covers all information related to an identifiable, living person and an identifiable, existing juristic person. The Act is suffused with individual autonomy and self-determination of individuals, regulates the processing of personal information, and safeguards individuals' rights to privacy. This extends to protecting against the unlawful collection, retention, dissemination and use of personal information. There are eight conditions ((*i*) accountability, (*ii*) processing limitation, (*iii*) purpose specification, (*iv*) further processing limitation, (*v*) information quality, (*vi*) openness, (*vii*) security safeguards, and (*viii*) data subject participation) which must be met when personal information is processed, and it is the responsibility of the responsible party (in the healthcare context either the practitioner or researcher) to ensure the lawful processing of personal information in a manner that does not infringe on the constitutional rights of individuals to privacy. Essentially, when personal information is collected for research purposes, a participant should know what type of information is being collected, why it is being collected, what will happen to the information, how long it will be retained, whether it will identify

the participant, if and why it will be shared, and whether it will be transferred outside SA and why.

Of significance to the use of AI technology is section 71 of POPIA which contains a general prohibition against the processing of personal information by automated means taken without human oversight or intervention. With automated decision making becoming much easier, where algorithms and AI enable speedy decision making, data subjects have the right to question significant decisions that have been made on a solely algorithmic basis. POPIA provides for protection in this instance, which is welcomed, especially when we consider how AI can be prone to pre-existing biases.[13] When we consider the transfer of data, section 72 of POPIA becomes applicable and provides an added layer of protection. National transfers of data may take place with informed consent and appropriate ethics review. International transfers may take place under five circumstances, three of which appear relevant for research purposes; however, only one ground appears to be practical, which is when the recipient in the foreign country is subject to a law, binding corporate rules or binding agreement that provides for an adequate level of protection that upholds principles that are substantially similar for the processing of personal information (section 72(1) of POPIA). A binding contractual agreement, e.g. a data transfer agreement (DTA) that upholds the principles for the processing of personal information as set out in POPIA, seems to provide a realistic solution for the transfers of personal information outside our borders.

With regard to cybercrimes, Smith J in *Msomi v S* offered the following explanation:

> … cyber-crimes have far-reaching consequences for the economy and the public, and courts must impose sentences that reflect the serious nature of the crimes. It is so that there is unfortunately a misguided perception that these crimes are somewhat less morally reprehensible than fraud and theft committed in the 'old fashioned' way. This perception is unfortunately further encouraged by films in which cyber-criminals are portrayed as debonair and devil-may-care rebels who fight a lone and just battle against an evil system. The reality is, however, far uglier. As is the case here, these types of crimes are more often than not motivated solely by greed, and not by any desire to do some societal good …The ability of cyber 'hackers' to infiltrate these electronic systems for their own selfish purposes consequently has far-reaching and deleterious consequences for the economy, both domestically and globally.[15]

From a data breach perspective, POPIA, which governs the processing of personal information, sets out offences (sections 100 - 106), penalties (sections 107 and 108) and fines (section 109) where its provisions are infringed and places a duty on responsible parties to disclose breaches. Data breaches are further safeguarded under the Cybercrimes Act 19 of 2020 and in the Electronic Communications and Transactions Act 25 of 2002. Prior to the Cybercrimes Act, the Electronic Communications and Transactions Act 25 of 2002 (ECTA) was the main piece of legislation that enabled and facilitated electronic communications and transactions in the public interest. The Cybercrimes Act, which offers comprehensive legislation dealing exclusively with cybercrimes and related issues, was signed into law in June 2021. While data protection and cybercrimes are two distinct areas of information communications technology, there is a correlation between these two areas in that the law now has an opportunity to remedy situations of vulnerability.[16] Considering the fact that data have been described as the 'new oil'[17] and noting that the commission of crimes across physical borders has become easier, further emphasises the relationship between laws relating to cybercrimes and data protection.[17]

Notably, in May 2024, the Department of Communications and Digital Technologies published the National Policy on Data and Cloud.[18] The policy recognises data as a strategic asset and acknowledges that the capacity to transform data into meaningful insights is currently largely confined to major technological companies in developed countries. Hence, there is a pressing need for SA to develop the capacity to fully exploit the opportunities presented by a data-driven economy (section 3). Key principles of the policy include: accelerating the rollout of digital infrastructure to ensure fast, secure, and reliable broadband connectivity; ensuring data privacy and security; promoting open data and data interoperability; and adopting a cloud-first approach (section 2). It applies to national and provincial government; organs of state or public enterprises; the private sector; general public or individual citizens; data controllers; and data custodians (section 11). The policy aims to guarantee the secure and reliable storage of data in the cloud, and protect personal and sensitive information from cyber-attacks by establishing data protection protocols, as required under POPIA (section 4). The policy further recognises the importance of the free flow of data as a catalyst for the global exchange and sharing of information and data and highlights that cross-border data transfers and sharing should be carried out in such a manner as to respect the security and sovereignty of SA (section 15.4). In addition, the policy recognises that SA is part of a globally connected and digitally transformed and transforming community and should therefore not only assert its data sovereignty rights but also adopt a cross-border data transfer regime that enables collaborative partnerships with regional, continental and other global partners (section 3). However, unlike the draft version of the policy which stipulated that all data generated in South Africa be considered the property of South Africa, irrespective of the location of the technology company, the final policy does not mention ownership rights in data. With regard to data breaches, the policy underlines the fact that although laws addressing cybercrimes and online-related crimes exist, there are challenges in preventing, investigating and prosecuting these crimes owing to a lack of human capacity and financial resources (section 15.3). In addition to adequately resourcing and capacitating data protection authorities to investigate, charge and prosecute individuals involved in data breaches, awareness campaigns should be conducted to empower citizens to understand and assert their rights concerning their data and educate citizens on where to report data breaches and other abuses or violations as outlined in POPIA, the Cybercrimes Act and any other related policies and legislation (section 15.3.1).

Thus, POPIA, the Cybercrimes Act, the ECTA and the National Policy on Data and Cloud form a network that attempts to balance privacy protections while promoting and recognising the immense value of open science, with SA having a key role to play in data-driven discovery. But it is not only SA laws and policies that have strengthened to improve privacy protections for personal information/data, but ethics guidelines have also evolved to extend protections to data generated in the care of patients in modern healthcare.

Ethical guideline reforms

The Health Professions Council Guideline on Confidentiality, Booklet 5, as revised in 2021,[19] increases the responsibilities on healthcare providers to ensure the safety of their patients' personal information. Another ethical guideline which recognises the privacy risks that come with the advent of new technologies which have driven a cultural transformation in the delivery of healthcare and more particularly for health research, is the South African Ethics in Health Research Guidelines – Principles, Structures and Processes

(2024) issued by the National Health Research Ethics Council (NHREC).[20] This is the third edition of the guidelines, which provides the minimum national benchmark of norms and standards for responsible and ethical conduct of research in SA. The guidelines recognise that data sharing raises specific ethical concerns in relation to privacy and that data-sharing decisions involve trade-offs between protecting privacy and advancing research. They provide guidance to researchers and research ethics committees (RECs) when the use and transfer of data is contemplated. They also reiterate the processing requirements set out in POPIA and advocate for the use of separate Material Transfer Agreements (MTAs) and DTAs (section 4.2.2). While the new guidelines are not perfect, it is currently the only document that attempts to steer the application of research ethics considerations to AI research proposals (section 3.4.4.1). If the researcher is focusing on machine capability and there are no human participants, then no ethical review and approval is needed. However, if the researcher intends to apply such technologies in a clinical setting and involves human participants, then ethics review is required.

Transparency, explainability, responsibility and accountability, equity and fairness, benefit sharing, safety and security, risk of harm, safety measures, and monitoring are some of the factors that researchers and RECs need to consider for AI research (section 3.4.4.1). In addition, the guidelines highlight that ethical scrutiny of AI research projects should be continuous and adapt to evolving circumstances. They also provide a set of 11 questions that RECs should consider during the review process, including whether the AI technology is appropriate and adaptable to the local context and what measures are in place to ensure that the rights and privacy interests of vulnerable groups included in AI research are protected. Another question for RECs to consider and which is relevant to the discussion on privacy, is what will happen to data after death of a participant/s; and how will safety of the information be maintained, and disclosure of the information facilitated (section 3.4.4.1)? The guidelines acknowledge that RECs will face many novel and complex issues when dealing with data science, and recommend that RECs should co-opt or appoint experts on data science, especially for technical input. Further, RECs should involve both researchers and data subjects in the assessment of BD research (section 3.4.4.2).

Although progress has been made towards the development of an ethico-regulatory framework that recognises broad privacy protections for individuals, translating protections into practice is particularly challenging when it comes to data in health research, considering the added challenges that AI brings to the table.

Recommendations towards a way forward

While we have progressed significantly in developing laws, policies and guidelines geared towards privacy protections, it is prudent to take a step back and remember the lessons learned from the historical exploitation on the continent, including the exploitation of human biological materials and apply the same efforts into translating data protection provisions into practice.

What we may benefit from are:

1. Careful efforts to ensure data security. For example: implementing strong access control measures, encrypting data, developing wide-ranging data security policies, adopting advanced security technologies to protect patient data, upgrade outdated technology to mitigate opportunities for potential hackers, detecting potential threats, shutting down systems immediately in case of an intrusion, removing compromised files, and preserving details of the breach for investigation which should be incorporated into a comprehensive incident report plan.
2. A national DTA template to manage the transfer of data across SA borders. Any practical data management tool that is developed to regulate data flows should be adapted in line with appropriate safeguards that respect the dignity of people, particularly considering the pre-democratic South African context. While some institutions already use DTAs and another has proposed a national template,[21] combining efforts into developing a nation-wide template will assist in streamlining processes for researchers, RECs and institutions.
3. Introducing a framework for the regulation of AI which speaks to the best interests of all people. To this end, the Department of Communications and Digital Technologies published the SA National Artificial Intelligence Policy Framework[22] in August 2024, towards the development of a national AI policy.
4. Engagement with communities and community healthcare leaders to accelerate Fourth Industrial Revolution (4IR) technology adoptions and education for the general public to familiarise population groups with existing technology and future expectations.
5. Upskilling RECs to equip members to deal with protocols that involve BD and the use of AI technology. Many of the challenges faced by RECs seem to centre on safeguarding the privacy of research participants. This focus often overshadows the need to balance protecting participant privacy and fostering research and scientific advancement, which in turn depends on increased data sharing.[23]
6. Establishing clarity around the ownership of data, which would in turn develop trust among institutions and participants that their data will be used only for the purposes with which they intend. This can also create certainty regarding how much control institutions and participants have over their data, which may assist in countering 'digital colonialism'.
7. A serious obstacle to the uptake of the development of AI in Africa is the availability of data and the costs associated with its acquisition. Therefore, directed investment including capacity building at a national and regional level, development of digital infrastructure, and accessibility to internet (use and coverage) is crucial.

Conclusion

Broadly, privacy governance in SA has progressed at a rapid pace, from the inclusion of privacy as a fundamental right within the Constitution (1996), to the development of legal and ethical safeguards for the processing for personal information and advancing a framework to manage cybercrimes. SA has made notable progress towards establishing a comprehensive ethico-regulatory framework as a foundation, designed to safeguard the privacy and confidentiality of patients and research participants' data within the healthcare sector. However, the challenge lies in effectively implementing privacy protections in a way that balances safeguards against the growing need for SA to flourish in the era of open science. In addition, AI advancements present considerable challenges that the country must address as it works towards striking this balance. Furthermore, the rise in local data breaches, especially within the healthcare sector, underscores the urgent need to translate paper into practice by strengthening systems and enforcing the ethico-legal framework governing the processing of data in SA, including ways in which to efficiently handle its misuse. This involves ensuring the adoption of ethically sound practices, adaptable infrastructure, and robust governance that is specific to the SA context.

Declaration. None.

Acknowledgements. This article was adapted from a presentation titled *Data privacy and protection in AI driven healthcare* provided by the author at the SAMA roundtable in AI, during November 2024.

Author contribution. Sole author.

Funding. None.

Conflicts of interest. None.

1. Alder S. Healthcare data breach statistics. HIPAA J. 2024. https://www.hipaajournal.com/healthcare-data-breach-statistics/ (accessed 11 September 2024).
2. Check Point Research. Average weekly global cyber-attacks peak with the highest number in 2 years, marking an 8% growth year over year. 2023. https://blog.checkpoint.com/2023/07/10/average-weekly-global-cyber-attacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year/ (accessed 11 September 2024).
3. Majola G. Cyber-attacks target agriculture, govt services in Africa: Mimecast report. IOL. 26 August 2024. https://www.iol.co.za/business-report/economy/cyber-attacks-target-agriculture-govt-services-in-africa-mimecast-report-ec563d33-0fc3-4d86-acac-ece37b4d32cc (accessed 11 September 2024).
4. Brederode W. All systems down as cyber-attack hits govt's national health lab. News24. 2024. https://www.news24.com/fin24/companies/all-systems-down-as-cyber-attack-hits-govts-national-health-lab-20240412 (accessed 11 September 2024).
5. Illidge M. South African mining giant hacked. MyBroadband. 9 February 2024. https://mybroadband.co.za/news/security/482123-south-african-mining-giant-hacked.html (accessed 9 February 2024).
6. Illidge M. 'BlackSuit' behind attack on critical South African healthcare service. MyBroadband. 2024. https://mybroadband.co.za/news/security/488456-blacksuit-behind-attack-on-critical-south-african-healthcare-service.html (accessed 11 September 2024).
7. Francke RL. All operations restored at NHLS, following cyber attack. IOL. 2024. https://www.iol.co.za/news/south-africa/all-operations-restored-at-nhls-following-cyber-attack-20240315 (accessed 11 September 2024).
8. Palmer K. Taylor & Francis AI deal sets 'worrying precedent' for academic publishing. Inside Higher Ed. 2024. https://www.insidehighered.com/news/2024/08/10/taylor-francis-ai-deal-sets-worrying-precedent-academic-publishing (accessed 11 September 2024).
9. Vayena E, Blasimme A. Biomedical big data: new models of control over access, use, and governance. Bioethical Inquiry 2017;14:501-513.
10. Naidoo S, Bottomley D, Naidoo M, Donnelly D, Thaldar DW. Artificial intelligence in healthcare: Proposals for policy development in South Africa. S Afr J Bioeth Law 2022;15(1):11-16. https://doi.org/10.7196/SAJBL.2022.v15i1.797
11. World Health Organization. Ethics and governance for artificial intelligence in health. Geneva: WHO; 2021.
12. Zhang Q, Gao J, Wu JT, Cao Z, Zeng D. Data science approaches to confronting the COVID-19 pandemic: A narrative review. Phil Trans R Soc A 2021;380:20210127.
13. Van Noorden R, Perkel JM. AI and science: What 1,600 researchers think. Nature. 2023. https://www.nature.com/articles/d41586-023-02740-6 (accessed 11 September 2024).
14. Klang E, Tessler I, Freeman R, Sorin V, Nadkarni GN. If machines exceed us: Health care at an inflection point. NEJM AI 2024;1(10). https://doi.org/10.1056/AIp2400559
15. Msomi v S (39/2018) [2019] ZAECGHC 80; 2020 (1) SACR 197 (ECG) (3 September 2019) at para 34.
16. Snail ka Mtuze S. The convergence of legislation on cybercrime and data protection in South Africa: A practical approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013. Obiter 2022;43(3):539.
17. Habl CA, Hummer M, Maier G. Data is the new oil: How COVID-19 boosted information transparency in Austria. Eur J Public Health 2021;31(Suppl 3).
18. Department of Communications and Digital Technologies. National Data and Cloud Policy. South Africa: Government Gazette No. 5074; 2024. https://www.gov.za/documents/electronic-communications-act-national-data-and-cloud-policy-5074-2024-05-20 (accessed 11 September 2024).
19. Health Professions Council of South Africa. Guidelines on confidentiality: Protecting and providing information. Booklet 5. 2021. Pretoria: HPCSA; 2021. https://www.hpcsa.co.za/Uploads/Professional_Practice/Booklet_5_Confidentiality_Protecting_and_Providing_Information_vDec_2021.pdf (accessed 11 September 2024).
20. National Health Research Ethics Council. South African ethics in health research: principles, processes and structures. 3rd ed. Pretoria: National Department of Health; 2024.
21. Thaldar D, Botes M, Swales L, Esselaar P. Enhancing data governance in collaborative research: Introducing SA DTA 1.1. S Afr J Bioeth Law 2024;17(2):e2300. https://doi.org/10.7196/SAJBL.2024.v17i2.2300
22. Department of Communications and Digital Technologies. South Africa National Artificial Intelligence Policy Framework. 2024 https://policyvault.africa/south-africa-national-artificial-intelligence-ai-policy-framework-2024 (accessed 11 September 2024).
23. Mahomed S, Labuschaigne M. The evolving role of health research ethics committees in the era of open data. S Afr J Bioeth Law 2022;15(3):80-83.

Received 2 February 2025. Accepted 5 May 2025.