Overview of AI regulation in healthcare: A comparative study of the EU and South Africa

T Naidoo, LLM (Medical Law)

College of Law and Management, School of Law, University of KwaZulu-Natal, Pietermaritzburg, South Africa

Corresponding author: *T Naidoo (theshaya1826@gmail.com)*

This article provides a comparative analysis of the regulatory landscapes governing artificial intelligence (AI) in healthcare in the European Union (EU) and South Africa (SA). It critically examines the approaches, frameworks and mechanisms each jurisdiction employs to balance innovation with ethical considerations, patient safety, data privacy and accountability. The EU's proactive stance, embodied by the AI Act, offers a structured and risk-based categorisation for AI applications, emphasising stringent guidelines for risk management, data governance and human oversight. In contrast, SA's regulatory environment is characterised by its infancy and lack of specificity, with existing legislation such as the National Health Act and the Medicines and Related Substances Act providing a foundational but limited framework for addressing the unique challenges posed by AI in healthcare. The article delves into the dynamic nature of AI technologies, highlighting the need for continuous risk assessment, the importance of transparent and responsible data governance and the critical role of human oversight in ensuring patient safety and autonomy. It discusses the obligation of clear liability frameworks to address potential malfunctions and security breaches in AI applications. Through this comparative lens, the manuscript identifies regulatory gaps and proposes that the South African Law Reform Commission (SALRC) should play a predominant role in developing draft legislation for AI prior to the evolution of challenges related to these technologies.

Keywords. regulation, healthcare, innovation, accountability, privacy.

S Afr J Bioethics Law 2024;17(3):e2294. https://doi.org/10.7196/SAJBL.2024.v17i3.2294

In the evolving landscape of healthcare, the integration of artificial intelligence (AI) has the potential to transform the operation of industry and revolutionise diagnostics, treatment and patient care.[1] However, harnessing these potentials imposes comprehensive regulatory frameworks that can sustainably balance innovation with ethical considerations, specifically in the context of patient safety, data privacy and accountability.[2] The primary focus of this comparative article is to consider the contrasting approaches to AI regulation in healthcare between the European Union (EU) and South Africa (SA), focusing on the divergent strategies, legislative frameworks and enforcement mechanisms.

This research is inspired by the flagship EU AI Act (AI Act), unanimously endorsed by the ambassadors of the 27 EU member states, which aims to scrutinise the nuanced differences and potential implications of the adoption and oversight of AI technologies within the context of healthcare ecosystems.[3] The AI Act is personified by its active approach that prescribes stringent guidelines for risk management, data governance and human oversight.[4] In contrast, SA's regulatory framework lacks specific regulations and dedicated enforcement mechanisms such as designated regulatory bodies, clear enforcement procedures and responsible officials.

Regulatory landscape overview

While AI regulation in SA is in its early stages,[5] academics have acknowledged the requirement for tailored regulatory frameworks, specifically in high-risk areas such as healthcare. Donnelly[6] has explained the challenges and guiding principles associated with the regulation of AI in SA, with a subsequent study emphasising that conventional legislative frameworks should be supplemented with specialised legal and medical frameworks to address AI's healthcare impacts effectively.[7] Donnelly's focus on healthcare suggests a potential gap in current efforts. While foundational principles are crucial, they may not suffice. Tailored regulations, as in other high-risk sectors, may be more appropriate to address the unique risks and considerations in healthcare to ensure responsible AI development and use.

From a healthcare perspective, academics have acknowledged the challenges that may potentially impede the integration of AI into existing healthcare systems. These challenges include the need for ethical and policy considerations before implementing regulations, ensuring precise data quality, privacy, transparency of algorithms and addressing issues of social and distributive justice in AI design, development and deployment.[8] In SA, these challenges are compounded by outdated legislation and concerns about the adverse impact of widespread AI applications on healthcare workers.[9] The challenges manifest in various dimensions, with some employees facing redundancy owing to automation,[10] as AI has the potential to assume tasks presently executed by human workers. Others may be concerned about the introduction of novel intricacies into their operational frameworks, imposing the acquisition of entirely new skill sets to collaborate with these intelligent systems effectively.[11]

In a comparable scenario, there is uncertainty regarding assigning liability, as the conventional fault-based framework often used in medical negligence cases may not adequately address harm stemming from emerging technologies, mainly when the fault is unclear.[12] From a SA perspective, challenges like poor infrastructure and unequal access to resources will likely hinder the widespread adoption of AI in healthcare. For example, limited access to stable electricity and internet connectivity, particularly in rural areas, poses obstacles to deploying and maintaining AI-driven systems. The gap between urban and rural populations may be exasperated by socioeconomic disparities, thus facilitating unequal distribution of healthcare resources.

However, academics have proposed various solutions for managing potential liability associated with AI in a healthcare context.[13] One suggestion involves attributing personhood, though this approach is controversial because of the practicality and consequences of considering AI as a legal entity accountable for its actions, challenging conventional concepts of legal identity and responsibility.[14] Judicially, while AI itself cannot currently be sued, potential avenues include holding developers or owners accountable for AI actions, akin to pet owners being liable for their pets. However, the precise manner for integrating AI into lawsuits remains unclear, as these technologies are not implicated directly in legal cases against their creators or owners.

From a broader perspective, if AI were legally recognised as a person, the judicial process would encompass unique considerations. One potential approach could involve treating AI similarly to corporations, which are legal entities capable of being sued. Practically, AI could be cited in a summons through their designated legal representation or registered agent. In other words, similar to how corporations have designated individuals to represent them in legal matters, AI could have appointed agents or legal guardians to represent its interests in court. These representatives would act on behalf of the AI, responding to summonses and participating in legal proceedings as required by law.

A relevant example of innovation in this context is SA granting a patent with AI (DABUS) as the inventor. This has introduced broad challenges regarding legal personhood, intellectual property rights and the broader consequences of attributing inventorship to non-human entities. It demonstrates the complexities and potential impediments that may arise from recognising AI as a legal entity, emphasising the need for carefully curated regulatory frameworks.[15] As previously noted, there is controversy surrounding AI's legal personhood. However, the recognition of AI as an inventor introduced fundamental questions regarding responsibility and accountability: If AI creates something novel, who owns the rights to that creation? Moreover, if the invention causes harm or infringement, who bears the legal responsibility—the AI, its developers or the entity that deployed it? There are also ethical and moral consequences, as acknowledging AI as an inventor could undermine human creativity in innovation and potentially devalue the contributions of human inventors.[16]

A parallel approach involves the assignment of accountability to the physician through the principal-agent relationship, which potentially risks impeding AI-integrated healthcare devices owing to the potential liabilities imposed on medical practitioners. However, it must be acknowledged that rising medico-legal claims[17] in SA have led medical practitioners to perceive this liability as significant. These escalating claims can adversely impact the medical community, dissuading doctors from practising medicine freely owing to soaring insurance premiums and fear of litigation. This effect may be exacerbated by increasing physicians' perceived accountability and caution, potentially hindering the widespread adoption of AI tools. Hence, alternative approaches such as fostering shared responsibility between doctors, hospitals and AI developers, must be explored, as relying solely on physicians may not effectively address the complexities of medico-legal challenges.

A regulatory approach that has been briefly explored is the application of product liability legal frameworks, specifically the Consumer Protection Act (CPA) in SA. However, this approach has been criticised because of the dynamic nature of AI technologies, which often extends beyond the conventional definition of product defects, thereby blurring the lines of accountability and complicating the determination of the root causes of harm. Similarly, in the context of remedies for strict liability, it has been proposed to simplify the compensation process by shifting focus to the harm caused rather than proving fault. Another alternative is dispute resolution, which emphasises resolving conflicts and facilitating regulatory sandboxes, as opposed to assigning blame.

Based on the above proposed solutions, it is suggested that a reconciliatory approach prioritising dispute resolution and the facilitation of regulatory sandboxes could offer the most pragmatic solution by focusing on conflict resolution and fostering an environment conducive to innovation. This strategy could mitigate AI-related liabilities while fostering progress in healthcare. Essentially, a balanced approach that primarily focuses on reconciliation underpinned by robust regulatory oversight, is advisable to effectively address the challenges posed by AI in healthcare, ensuring both accountability and innovation thrive in tandem.

While South Africa's Policy Action Network (PAN) highlights the need for skilled healthcare workers and the upskilling of personnel to effectively use digital health technologies, it has been established that current policy frameworks do not adequately foster innovation in the application of AI in healthcare. Hence, it is essential to establish practical and solution-oriented policy guidance, drawing from international policies and guidelines such as the United Nations Educational, Scientific and Cultural Organization (UNESCO) recommendation on the ethics of AI,[18] the Group of 20 (G20) AI principles[18] and the development of a national policy framework that outlines guiding principles to address the challenges posed by AI in healthcare.

In SA, the National Health Act 61 of 2003 is a prominent legislative framework governing healthcare services and related matters. However, its primary focus is on ensuring the quality and accessibility of healthcare, and it lacks explicit directives regarding the express integration and regulation of AI technologies. Consequently, it is proposed that while the CPA offers a streamlined, patient-centric approach, its broad nature may not fully address the unique complexities of healthcare such as informed consent and doctor-patient trust. The Act's emphasis on consumer rights may also facilitate defensive medicine practices, where healthcare providers prioritise avoiding legal issues over delivering optimal patient care.

Consequently, the ideal solution may involve a multifaceted approach. Strengthening the National Health Act (NHA) with consumer protection principles specific to AI in healthcare can provide a solid foundation. However, targeted regulations for emerging technologies such as AI must be integrated to ensure appropriate safeguards. Clear guidelines should also be implemented to outline the application of the CPA in high-risk areas such as healthcare. The primary goal would be to empower patients and ensure fair practices while preserving the vital doctor-patient relationship and fostering innovation.

Similarly, the Medicines and Related Substances Act (MRSA) No. 101 of 1965 may be considered. The MRSA regulates the registration of drugs, establishment of the Drugs Control Council and medical devices in SA, with amendments made in 2008 and 2005. The Act defines a medical device as 'any instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article…'. This definition can include AI medical devices protected by the MRSA and bound by the prescribed requirements. However, any general software that falls outside the ambit of this definition in the context of healthcare applications would not be considered a medical device. This position is opposed by Kirby,[20] who argues that if an AI model is designed to examine or adapt anatomy or physiological processes, it could be classified as a medical device under the MRSA.

From a data protection perspective, the Protection of Personal Information Act 4 of 2013 (POPIA), which came into effect in 2021, addresses the protection of individuals' personal information. This Act has significant consequences for data use, access and transfer, including strict requirements for obtaining consent from data subjects, ensuring data security through appropriate measures and providing mechanisms for individuals to access and correct their information. Consequently, it becomes necessary to integrate safeguards aimed at preventing unauthorised access and data breaches, ensuring compliance with regulations and upholding data protection standards in recipient jurisdictions. The primary aim is to mitigate risks and enhance transparency in the context of personal data within AI systems. Consumers are also somewhat protected from potential risks associated with AI through the CPA. The Act classifies the protection of consumer interests within distinct contexts and with varying degrees of specificity. The primary purpose of CPA is to protect consumer rights, emphasising transparency, disclosure and accountability in consumer transactions.[20]

Similarly, The National Health Insurance (NHI) Act presents both opportunities and challenges for AI in healthcare. AI has the potential to enhance data management and patient care under the NHI, which raises concerns regarding the management of sensitive health data in compliance with POPIA. Thus, transparent guidelines are needed to balance data protection with AI capabilities. In an ethical context, the National Health Research Ethics Council (NHREC) Ethics Guidelines 2024 provide a framework for AI application in health research, focusing on transparency, fairness and accountability. Further, the Department of Communications and Digital Technologies (DCDT) Draft Discussion Document on South African AI policy outlines essential considerations that are necessary for AI integrations, including its impact on data protection and healthcare delivery. Consequently, a comprehensive policy approach is necessary to reflect AI advancements with national healthcare objectives and data security regulations.

The EU landscape

In stark contrast to SA, AI in healthcare in the EU is specifically regulated by the European Union's Artificial Intelligence Act (AI Act), 2023. The AI Act aims to ensure the safe, transparent and responsible application of AI within the region, prioritising citizen protection and promoting innovation while addressing the risks associated with AI models. The European Medicines Agency adopts a human-centric approach, prioritising compliance with existing legal requirements, ethics and respect for fundamental rights.[21] It is proposed that comparing this Act to SA's current regulatory landscape is necessary to highlight critical areas for improvement and adaptation. The Act serves as a model for a progressive, structured approach to AI regulation, offering valuable insights into potential amendments SA may adopt in its regulatory framework. Therefore, understanding the EU's comprehensive strategies as a benchmark is crucial for SA to address gaps in existing laws such as the NHA and the MRSA. This comparative analysis aims to underscore the need to enhance SA's regulations to align with international best practices and effectively address the emerging challenges posed by AI technology.

Broadly, the AI Act categorises AI systems based on their risk levels,[22] with tiered oversight and requirements mandated based on potential risks posed by the technology. In medical contexts, AI is classified as high-risk, requiring a comprehensive assessment before being introduced to the public, followed by periodic evaluations throughout its lifecycle. High-risk AI systems are further defined as AI systems integrated into products that are regulated by the EU's product safety legislation such as medical devices and lifts, as well as AI systems applied in critical areas like the management and operation of infrastructure, education, employment, law enforcement, migration, asylum and border control and AI systems that facilitate legal interpretation and application of the law.[23] As a high-risk AI system, medical devices, as per Article 5 of the AI Act, must comply with strict obligations such as mandatory Fundamental Rights Impact Assessments and Conformity Assessments.

The AI Act mandates comprehensive risk management in Article 46, requiring an assessment of potential risks throughout the lifecycle of the device, from conception to deployment, maintenance and decommissioning. Articles 47 to 51 further emphasise responsible data governance focusing on transparency, fairness and robust data security measures. These provisions ensure that the data used to train and operate the AI system are of high quality, accurate and up-to-date, integrating diverse datasets to mitigate bias. Continuous updates to the data are required to reflect evolving medical knowledge, along with rigorous quality checks to guarantee accuracy.[24] Patients have the right to understand how the data are collected, used and stored. They must be provided with clear information on data practices, comprehension of how AI decisions are made and mechanisms to address potential bias in algorithms, which are essential to ensure transparency and fairness.[25]

Automated decision-making (ADM) becomes relevant in this context, with Section 71 of POPIA addressing ADM and its impact on individuals. This section reflects the right of patients to understand the application of AI in their care. POPIA also indirectly compels responsible parties such as healthcare providers to consider potential bias in algorithms by mandating that patients be provided with 'sufficient information about the underlying logic' used in their specific case. This allows patients to identify and potentially challenge biased decisions. However, it is important to note that POPIA does not explicitly require an explanation of the inner workings of complex algorithms. Instead, the primary focus of section 71 is ensuring the patient understands how the decision affects them and whether they have recourse.

Article 52 of the AI Act further acts as a paramount safeguard against potential AI risks. This article requires the technical ability of AI medical devices to be manually overridden or adjusted by healthcare professionals when necessary, enabling them to review or modify AI-based diagnoses. It requires clear procedures for human intervention in the event of a system malfunction.[26] Thus, definite boundaries of accountability must be established to specify who is responsible for the operation of these functionalities of the AI system to ensure transparency.[27]

The issue of liability and security is addressed in Article 53 by requiring that the AI component of a medical device functions as intended and undergoes rigorous testing and validation procedures. This includes consistent monitoring for performance degradation, vulnerability assessments and periodic patching of identified security flaws, ensuring the integrity of the AI system. Meanwhile, Article 54 further emphasises the need to consistently acknowledge and address potential concerns through regular monitoring of key performance indicators to detect any decline in performance or unforeseen outcomes. Feedback collection from impacted healthcare professionals is encouraged to identify potential issues from their perspective, promoting awareness and improvement in the system.[28] The primary aims of transparency and accountability in the AI Act are further emphasised by this article, which mandates the monitoring of the performance of the device after deployment to facilitate efficient identification and mitigation of any emerging risks or unintended consequences.

Comparative analysis

As established above, the main goal of the AI Act is to regulate high-risk AI systems based on specific criteria. In contrast, the SA legislative framework currently lacks explicit provisions tailored to AI in the context of healthcare, primarily encompassing broader sectors. From a healthcare perspective, Donnelly[6] has proposed three legal impediments to the implementation of effective AI regulations: the registration processes of new AI health technologies, the ethical framework of these emerging technologies and the applicable legal principles that regulate liability when patients or users of these technologies are harmed. While various facets of the healthcare sector have begun integrating AI applications such as automated dispensing machines, which are regulated under the South African Pharmacy Council's Good Pharmacy Practice Standards (GPP Standards)[29], it is clear that a more comprehensive regulatory strategy specifically targeting AI software is necessary. This strategy should facilitate assessment and supervision from development to the operational stages.

While the MRSA lacks explicit provisions analogous to the AI Act, its objectives are to ensure the safety, efficacy and quality of medicine, including those used in AI-powered diagnostics or treatment algorithms. This reflects the goal of the AI Act of ensuring high-risk AI systems function as intended and do not pose undue risks to individuals. The MRSA further regulates the manufacture, advertising and distribution of medicines, which directly influences the quality of data used in AI development by ensuring that medicines used for training or analysis are controlled and fulfil specific prescribed standards.

While the impact of this Act on AI is not explicitly reflected in its provisions, the MRSA regulates medical devices that perform autonomous tasks through the application of AI. The Act's definition of 'medical device' can be interpreted to include AI medical devices, but its general classification of software does not extend to AI-integrated medical devices, potentially leaving critical AI-driven tools unaddressed. The interpretation of medical devices suggested by Kirby[20] further introduces ambiguity and differentiated perspectives on AI classification. Section 23 of the Act further facilitates the establishment of the South African Health Products Regulatory Authority (SAHPRA) and the licensing of manufacturers and importers of active pharmaceutical ingredients. SAHPRA has not registered AI-related medical devices.

However, this is not directly equivalent to the AI Act's specific focus on data quality for AI development. While the MRSA does not directly address data governance and fairness in AI, it serves as a foundation for regulating medicines used in healthcare. Notably, neither Act comprehensively addresses the intricate challenges of AI in healthcare, including managing AI-related risks.

The CPA align most closely with Article 46 of the AI Act, which classifies the protection of consumer interests within distinct contexts and with varying degrees of specificity but fails to consider the impact of AI on these practices explicitly. However, Section 61(1) of the Act does establish strict liability for harm emanating from the supply of unsafe goods, with the Act only being applicable and enforceable when unsafe goods pose a risk of personal injury or property damage owing to a characteristic, failure, defect or hazard.[30] The introduction of 'strict liability' under Section 61(1) of the CPA is potentially contentious. While it establishes harm caused by unsafe goods, available defences can negate this strictness. In other words, liability can be avoided by a supplier if they can prove they were unaware of the defect and could not reasonably have discovered it through proper procedures. In this instance, an element of fault is introduced, thus making it more challenging to establish clear-cut strict liability uniformly. The complexity involved in proving a direct causal link between the defective product and the harm suffered can be complex, especially with AI technologies further complicating claims based solely on strict liability under the CPA.

Despite the modified form of strict liability under the CPA, the individual experiencing harm is still required to demonstrate a clear causal link between the harm suffered and the defect. However, the inherent opacity and complexity of AI decision-making make proving defects in AI systems challenging. The AI Act addresses this by promoting transparency, accountability and risk management within the development and deployment of AI systems.

For example, Article 13 mandates disclosure of decision-making processes in high-risk AI systems through techniques like feature importance analysis or decision trees specified in Annex III, which encourage the detection of biases or errors and enhance trust in AI applications. Article 10 requires ongoing risk management throughout the AI lifecycle, urging entities to identify, assess and mitigate risks, thus reducing the likelihood of harm caused by defects. Additionally, Article 22 grants individuals the right to an explanation for impactful AI-driven decisions. As a result, users are empowered to comprehend and challenge such decisions if required, as prescribed in Article 23.

It is proposed that healthcare practitioners use contractual clauses to limit liability arising from the application of AI software, but this approach may be detrimental to the interests of all parties and erode public trust. These clauses are widely considered unfair, unreasonable or unjust to healthcare users, contrary to the provisions of the CPA. The CPA term 'grey listed' refers to terms and conditions that are not outright prohibited or deemed unfair but are subject to scrutiny for potential unfairness to consumers. In AI applications, concerns are rising as these applications increasingly impact consumers across industries—from personalised pricing and targeted advertising to automated credit scoring and loan approvals.

Consequently, there is potential for these terms to be amended to address ambiguous AI-related terminology and adapt consumer protection laws to the realities of the digital age. As AI becomes more prevalent in consumer transactions, it is increasingly recognised that traditional consumer-protection frameworks may not adequately address the unique challenges posed by these technologies. Article 8 of the AI Act considers a broader range of AI-related risks, covering potential harm to fundamental rights such as privacy, non-discrimination and safety, as well as algorithmic bias leading to unfair decisions and societal wellbeing. This broader perspective adopted by the AI Act more accurately reflects the unique challenges posed by complex AI technology.

The difficulty of proving causality in AI systems is addressed in Article 10 of the AI Act, which mandates developers to maintain thorough records of an AI system's development process, training data and performance metrics. These data are essential for users or authorities to establish a causal link between harm and an AI system's malfunction, potentially addressing the challenges highlighted by the CPA. If one were to draw a direct comparison between the AI Act and the CPA, the practice of using contractual clauses to limit the liability placed on medical practitioners for AI-related harm could be challenged under Article 16 of the AI Act, which prohibits developers and users from relying on general terms and conditions to evade liability for AI systems causing harm.

Section 22 of the CPA could also be interpreted to extend to healthcare devices integrated with AI, as the CPA's core objective is to impose liability on suppliers for harm caused by defective products, fostering accountability in the marketplace. Section 22 mandates that suppliers provide comprehensive information to consumers for decision-making and protection against unfair business practices. While both Article 46 of the AI Act and the CPA prioritise consumer protection, the CPA offers a broad foundation for consumer rights across various sectors. In contrast, Article 46 offers detailed provisions explicitly addressing the complexities of AI in healthcare, thus establishing a benchmark for the regulation of AI systems in healthcare by emphasising the necessity of specialised ratifying frameworks to address emerging technological change, specifically when consumers are concerned.

While the primary focus of the CPA is product liability and consumer rights, the purview of the Act can be interpreted to apply to AI medical devices, which can be categorised as 'goods' in terms of the Act. For example, Section 61 explicitly addresses issues such as common malfunctions or security breaches stemming from the use of AI-infused medical devices. In such cases, the developer, manufacturer or healthcare provider may be held accountable. Thus, emphasising the importance of comprehensive design, testing, and consistent security measures for AI systems reflects the security emphasis of Section 54.

In the context of data governance, Articles 47 to 51 of the AI Act align with section 27 of POPIA, which prohibits the sharing of health data (categorised as special personal information under the Act), except in specific circumstances such as when third parties may be exposed to risk, like in the diagnosis of HIV. Similarly, Section 52 of the AI Act establishes the foundation for the responsible management of data, mainly focusing on the significant use of personal health data. Consequently, POPIA compliance becomes crucial with this Act mandating measures such as data minimisation, informed consent, and safeguards against unauthorised access or processing—critical measures for mitigating AI-related privacy risks and giving patients control over their health data. From a healthcare perspective, the NHA establishes guidelines for healthcare provision, emphasising informed consent and patient rights. This means that for patients to maintain autonomy in AI-driven healthcare, they must understand how AI is involved in their care.

It is essential to address the distinct yet complementary components of the General Data Protection Regulation (GDPR) and the AI Act from a data protection and AI governance perspective. While the GDPR protects individuals' rights over personal data usage, the AI Act extends this protection by directly targeting AI systems' development, deployment and use. Further, the primary focus of the AI Act is the mitigation of specific risks inherent to AI, such as bias, discrimination and opaque decision-making processes, which are not explicitly covered by the GDPR. Further, by prescribing precise compliance requirements for high-risk AI systems and emphasising the necessity of human oversight throughout the AI lifecycle, the AI Act provides a more nuanced and comprehensive framework for navigating the ethical and operational complexities of AI technology within the EU.

In addition to POPIA, the Cybercrimes Act plays a key role in creating a comprehensive framework for protecting sensitive patient data processed by AI medical devices. While POPIA addresses civil liability and regulates personal data protection, the Cybercrimes Act focuses on criminal offences related to data breaches. By referencing aspects of POPIA, the Cybercrimes Act works in tandem with it, establishing a comprehensive framework for safeguarding sensitive patient data handled by AI medical devices, covering both civil and criminal aspects of data protection.

POPIA emphasises preventive measures intended to mitigate security risks to personal information. When comparing this regulatory framework to the EU's approach outlined in the AI Act, there are some similarities and differences. The EU AI Act emphasises the compulsion of data protection and security in AI systems by requiring AI developers and users to comply with certain transparency, accountability and data protection requirements.

Conclusion

The EU's legislation demonstrates a proactive stance towards addressing the challenges posed by high-risk AI applications in a healthcare context, while SA's regulatory framework appears to be lagging. Existing frameworks such as the NHA and the MRSA provided the foundation, but they lack explicit provisions for the nuanced challenges posed by AI technologies in a healthcare context. Consequently, SA's regulatory framework would benefit from proactive legislative updates and comprehensive stakeholder consultations to develop a more nuanced and compelling legal structure. This approach will help foster an environment conducive to responsible and ethical AI development, ensuring patient safety and privacy. The primary goal is to harness the transformative potential of AI to enhance healthcare delivery while ensuring robust protections for patients in an increasingly AI-driven landscape.

Regulatory sandboxes may be an appropriate solution to bridge these gaps, allowing for controlled experimentation with AI technologies and providing a structured environment to assess new approaches while simultaneously mitigating risk. Similarly, transparent, robust principles for AI integration must be prioritised, primarily focusing on transparency, accountability and patient-centric considerations aimed at guiding the responsible deployment of AI technologies.

Declaration. None.
Acknowledgements. None.
Author contributions. Sole author.
Funding. None.
Data availability statement. Not applicable.
Conflicts of interest. None.

1. Alowais SA, Alghamdi SS, Alsuhebany N, et al. Revolutionizing healthcare: The role of artificial intelligence in clinical practice. BMC Med Educ 2023;23(1):689. https://doi.org/10.1186/s12909-023-04698-z
2. Mennella C, Maniscalco U, De Pietro G, Esposito M. Ethical and regulatory challenges of AI technologies in healthcare: A narrative review. Heliyon 2024;10(4):e26297. https://doi.org/10.1016/j.heliyon.2024.e26297
3. Simmons & Simmons. The EU AI Act. Available online https://www.simmons-simmons.com/en/publications/clsixo6nj0056ti9sb46qohpv/the-eu-ai-act-what-employment-lawyers-and-hr-personnel-need-to-know (9 June 2024).
4. Enqvist L. 'Human oversight' in the EU artificial intelligence act: What, when and by whom? Law Innovation Technol 2023;15(2):508-535. https://doi.org/10.1080/17579961.2023.2245683
5. Pedro F, Subosa M, Rivas A, Valverde P. Artificial intelligence in education: Challenges and opportunities for sustainable development. 2019. https://hdl.handle.net/20.500.12799/6533
6. Donnelly DL. First do no harm: Legal principles regulating the future of artificial intelligence in health care in South Africa. Potchefstroom Electron Law J 2022;25(1):1-43. https://doi.org/10.17159/1727-3781/2022/v25i0a11118
7. Laptev VA, Ershova IV, Feyzrakhmanova DR. Medical applications of artificial intelligence (legal aspects and future prospects). Laws 2021;11(1):3. https://doi.org/10.3390/laws11010003
8. Townsend BA, Sihlahla I, Naidoo M, Naidoo S, Donnelly DL, Thaldar DW. Mapping the regulatory landscape of AI in healthcare in Africa. Front Pharmacol 2023;14:1214422. https://doi.org/10.3389/fphar.2023.1214422
9. Naidoo S, Bottomley D, Naidoo M, Donnelly D, Thaldar DW. Artificial intelligence in healthcare: Proposals for policy development in South Africa. S Afr J Bioethics Law 2022;15(1):11-16. https://doi.org/10.7196/sajbl.2022.v15i1.797
10. Pham QC, Madhavan R, Righetti L, Smart W, Chatila R. The impact of robotics and automation on working conditions and employment. IEEE Robotics Automation Mag 2018;25(2):126-128. https://doi.org/10.1109/mra.2018.2822058
11. Morandini S, Fraboni F, De Angelis M, Puzzo G, Giusino D, Pietrantoni L. The impact of artificial intelligence on workers' skills: Upskilling and reskilling in organisations. Inform Sci 2023;26:39-68. https://doi.org/10.28945/5078
12. Martins HMG. Liability implications of artificial intelligence use in health: Fault and risk in public sector healthcare [dissertation]. Universidade Católica Portuguesa 2021. https://repositorio.ucp.pt/bitstream/10400.14/37674/1/202609898.pdf
13. Bottomley D, Thaldar D. Liability for harm caused by AI in healthcare: An overview of the core legal concepts. Front Pharmacol 2023;14:1297353. https://doi.org/10.3389/fphar.2023.1297353
14. Singh S. Attribution of legal personhood to artificially intelligent beings. Bharati Law Rev 2017;198. https://doi.org/10.58532/nbennurdtch4
15. Oriakhogba DO. Dabus gains territory in South Africa and Australia: Revisiting the AI-inventorship question. S Afr J Intellectual Property Law 2021;9(1):87-108. https://doi.org/10.47348/saipl/v9/a5
16. Lim D. AI & IP: Innovation & creativity in an age of accelerated change. Akron Law Rev 2018;52:813.
17. Prinsen L. Medicine and the law: The leading causes of medico-legal claims and possible solutions. S Afr Med J 2023;113(4):1140-1142. https://doi.org/10.7196/samj.2023.v113i4.134
18. Recommendation on the Ethics of Artificial Intelligence, United Nations Educational, Scientific and Cultural Organisation (UNESCO). 2021.
19. G20 Principles for Artificial Intelligence, endorsed by the G20 Leaders' Summit, Osaka, Japan, June 28-29 2019. Available from: https://oecd.ai/en/wonk/documents/g20-ai-principles (accessed 16 April 2024).
20. Kirby N. 'You, Robot'. Werksmans Attorneys Legal Brief (February 2018). https://www.werksmans.com/wp-content/uploads/2018/10/17659_Legal_Brief_Healthcare_FA.pdf. (accessed 19 March 2024).
21. Jacobs W, Stoop PN, Van Niekerk R. Fundamental consumer rights under the Consumer Protection Act 68 of 2008: A critical overview and analysis. Potchefstroom Electronic Law J 2010;13(3). https://doi.org/10.4314/pelj.v13i3.63675
22. European Medicine Agency. Reflection paper on the use of artificial intelligence in lifecycle medicines. Eur Med Agency. 2023. https://www.ema.europa.eu/en/news/reflection-paper-use-artificial-intelligence-lifecycle-medicines
23. European Parliament. EU AI Act: First regulation on artificial intelligence. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
24. Díaz-Rodríguez N, Del Ser J, Coeckelbergh M, de Prado ML, Herrera-Viedma E, Herrera F. Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics and key requirements to responsible AI systems and regulation. Inform Fusion 2023;99:101896. https://doi.org/10.1016/j.inffus.2023.101896
25. Wang C, Liu S, Yang H, Guo J, Wu Y, Liu J. Ethical considerations of using ChatGPT in health care. J Med Internet Res 2023;25:e48009. https://doi.org/10.2196/48009
26. Reddy S. Use of artificial intelligence in healthcare delivery. In EHealth-making health care smarter 2018. IntechOpen https://doi.org/10.5772/intechopen.74714
27. Palmieri S, Walraet P, Goffin T. Inevitable influences: AI-based medical devices at the intersection of medical devices regulation and the proposal for AI regulation. Euro J Health Law 2021;28(4):341-358. https://doi.org/10.1163/15718093-bja10053
28. Obasa AE, Palk AC. Responsible application of artificial intelligence in health care. S Afr J Sci 2023;119(5-6):1-3. https://doi.org/10.17159/sajs.2023/14889
29. South African Pharmacy Council (SAPC). Good Pharmacy Practice in South Africa. Pretoria: SAPC 2022.
30. Sihlahla I, Donnelly DL, Townsend B, Thaldar D. Legal and ethical principles governing the use of artificial intelligence in radiology services in South Africa. Dev World Bioeth 2023. https://doi.org/10.1111/dewb.12436

Received 5 June 2024. Accepted 2 October 2024