JUNE 2025

A STUDY ON DIGITAL HEALTH APPS IN SOUTH AFRICA: THE CASE OF MOM CONNECT, KENA HEALTH, ADA & LESSONS LEARNT

HFW REPORTS

Prepared By :

Lyla Latif (PhD)

HOUSE OF
FISCAL WISDOM

Nairobi, Kenya
www.house-of-fiscal-wisdom.org

Table of Contents

1. Introduction

The rapid proliferation of digital health technologies, particularly mobile health applications (mHealth apps), has fundamentally transformed the healthcare landscape in South Africa. These innovative tools promise to enhance accessibility, efficiency, and quality of care, aligning with the country's constitutional mandate to ensure progressive realisation of the right to health. However, the surge in health apps has also introduced complex legal and regulatory challenges that require critical examination. This study aims to provide a comprehensive legal analysis of the digital health ecosystem in South Africa, with a particular focus on the health app landscape. By adopting a multifaceted approach, the research delves into the legal and normative frameworks governing these digital interventions, the institutional governance structures involved, and the techno-legal factors shaping the development and adoption of health apps.

The study begins by mapping the existing legislative and regulatory environment in South Africa, exploring how the country's laws, policies, and standards accommodate and regulate the burgeoning digital health sector. This foundational analysis is crucial in identifying potential gaps, tensions, and areas for reform within the current legal framework. Building on this understanding of the regulatory landscape, the study then examines the institutional governance ecosystem responsible for overseeing the digital health landscape. The roles, mandates, and interactions of key governmental bodies, regulatory authorities, and professional associations are scrutinised to uncover the complexities and potential challenges in coordinating the governance of these emerging technologies. Recognising the pivotal role of various stakeholders in shaping the digital health ecosystem, the study subsequently explores the diverse actors, including public entities, private enterprises, international collaborators, and local communities, and their respective contributions and interests. This multi-stakeholder analysis illuminates the power dynamics, priorities, and potential tensions inherent in the development and deployment of health apps.

Building on this foundational understanding, the study delves into a detailed examination of the health app ecosystem in South Africa. By categorising the apps based on their functionalities and target user segments, the study provides a nuanced taxonomy to navigate the diverse landscape of digital health solutions. This taxonomic approach serves as a springboard for analysing the techno-legal factors that influence the financing, funding, and intellectual property arrangements underpinning the health app ecosystem. Finally, the study presents a comparative case analysis of three prominent health apps – MomConnect, Kena Health, and Ada – to illuminate the legal and regulatory implications of these digital health platforms. Through a combined literal and purposive analysis of their contractual terms and privacy policies, the study uncovers potential loopholes, risks, and challenges that warrant urgent attention from policymakers, regulators, and healthcare stakeholders.

2. Digital Health in South Africa

2.1. Mapping the Regulatory Environment

2.1.1. Laws, Regulations, Strategies and Standards

Section 27 of the **South African Constitution**[1], while not explicitly mentioning digital health, inherently supports the foundation for digital health policies through its broad mandate for the state to ensure access to healthcare as a basic human right. This section's requirement for the state to take 'reasonable legislative and other measures, within its available resources, to achieve the progressive realisation' of health rights implicitly embraces the adoption of modern technologies and innovations in healthcare delivery. One could argue that the digital health paradigm is a contemporary and effective means to fulfil the constitutional obligations under Section 27. As stated in the UN Special Rapporteur report, 'Digital innovation, technologies and the right to health' (A/HRC/53/65),[2] digital health initiatives by their nature aim to enhance accessibility, efficiency, and quality of healthcare services, thereby directly contributing to the progressive realisation of health rights. The Constitution's emphasis on equitable access to healthcare services aligns with the principles of digital health, which seeks to mitigate traditional barriers to care through technological solutions. Therefore, the constitutional mandate can be interpreted as not only accommodating but also necessitating the integration of digital health strategies into the broader framework of health rights realisation.

The **National Health Act 61 of 2003**, under Chapter 1 and Section 4, sets out the rights and duties pertaining to health services.[3] Section 74 provides the legal basis for establishing and maintaining a national health information system spanning public and private healthcare. This enables national policies and guidelines regarding e-health systems, telemedicine services, electronic health data exchange, and mobile health applications to improve access. However, additional provisions are needed to assure quality, interoperability, privacy and cybersecurity specifically for digital health. The **Health Professions Act 56 of 1974** establishes the Health Professions Council of South Africa (HPSCA) under Section 2 to regulate healthcare practitioners and protect the public.[4] The HPCSA's ethical rules and guidelines, as permitted under Section 49, have an oversight role when new care delivery models like telemedicine and mobile health are introduced. But being outdated, they require revisions incorporating digital health innovations to assure patient safety, privacy and continuity of care.

The **Protection of Personal Information (PoPIA) Act 4 of 2013** is a pivotal legislation governing how personal data, including medical records, are electronically processed.[5] PoPI advances principles of lawful processing, privacy and security which digital health systems must comply with

[1] Constitution of the Republic of South Africa, 1996, https://www.gov.za/documents/constitution/constitution-republic-south-africa-04-feb-1997

[2] UN, Digital innovation, technologies and the right to health' (A/HRC/53/65), https://www.ohchr.org/en/documents/thematic-reports/ahrc5365-digital-innovation-technologies-and-right-health

[3] Republic of South Africa, National Health Act, No 61 of 2003, https://www.gov.za/documents/acts/national-health-act-61-2003-23-jul-2004#:~:text=The%20National%20Health%20Act%2061,regard%20to%20health%20services%3B%20and

[4] Republic of South Africa, Health Professions Act, No 56 of 1974, https://www.sahpra.org.za/document/health-professions-act-1974-act-no-56-of-1974/

[5] Republic of South Africa, Protection of Personal Information (PoPI) Act 4 of 2013, https://www.gov.za/documents/protection-personal-information-act

under Sections 9-12. But enforcement measures and alignment with health regulations need strengthening considering increased data breaches. The **Electronic Communications and Transactions (ECT) Act 25 of 2002** under Section 42 enables valid exchange and storage of data messages and electronic transactions.[6] This permits electronic transmission of health records between systems, providers and patients. But additional provisions are necessary for securely sharing sensitive health information like genomic data electronically. The **Promotion of Access to Information Act 2 of 2000** empowers patients under Sections 14 and 51 to access their own medical records, including digitised versions from healthcare providers.[7] But does not explicitly require informed consent nor transparency from providers on how patient data is utilised within digital systems. Additional regulations are hence needed.

There are also two additional acts with relevant sections governing digital health in South Africa. The **Consumer Protection Act, 2008** sets out consumer rights concerning goods and services, without specifying technologies.[8] But under Sections 41 and 49, its prohibitions on false, misleading or deceptive claims regarding products' features, uses or benefits would be applicable to health apps and software marketed directly to public consumers. Hence it provides legal recourse regarding unverified wellness or diagnostic claims made through these digital health technologies even without expressly stating so. Similarly, the **Medicines and Related Substances Act, 1965** empowers the South African Health Products Regulatory Authority (SAHPRA) under Section 2 to regulate medical devices and IVDs without limiting to physical devices.[9] By implication, novel mobile medical apps that meet the medical device definition would thereby require SAHPRA approval prior to making diagnostic/treatment claims as per Sections 14-15 - despite the term app not being stated. This oversight ensures some level of efficacy and safety standards for software guiding clinical decisions.

The **National Digital Health Strategy for South Africa 2019-2024** further provides a comprehensive blueprint to leverage digital technologies to strengthen the country's health system.[10] It envisions 'better health for all South Africans enabled by person-centred digital health'[11] and sets strategic priorities like developing electronic health records, digitising health business processes, establishing integrated health information platforms, scaling up mobile health interventions, and building digital health workforce capabilities. Some key aspects of digital health covered in the strategy include governance structures, interoperability frameworks, electronic patient records, routine health information systems, mobile health initiatives, infrastructure and connectivity, capacity building, and regulatory provisions. The strategy notes successes like implementing standardised registers to improve data collection and establishing foundations for the National Health Insurance through the Health Patient Registration System.

Clear priority areas that are outlined in the strategy are finalising the unique patient identifier, achieving provider-patient interoperability, implementing standards testing for information systems, establishing data sharing agreements with private healthcare providers, developing the health electronic record, creating the digital health workforce, reducing connectivity costs, and strengthening the regulatory environment regarding data protection and cybersecurity laws. The strategy identifies

[6] Republic of South Africa, Electronic Communications and Transactions (ECT) Act 25 of 2002, https://www.gov.za/documents/electronic-communications-and-transactions-act

[7] Republic of South Africa, Promotion of Access to Information Act, No 2 of 2000, https://www.gov.za/documents/promotion-access-information-act#:~:text=The%20Promotion%20of%20Access%20to,protection%20of%20any%20rights%3B%20and

[8] Republic of South Africa, Consumer Protection Act, 2008, https://www.gov.za/documents/consumer-protection-act

[9] Republic of South Africa, Medicines and Related Substances Act, NO 101 of 1965, https://www.gov.za/documents/drugs-control-act-7-jul-1965-0000#:~:text=The%20Medicines%20and%20Related%20Substances,for%20matters%20incidental%20thereto.

[10] Republic of South Africa, Department of Health, 'National Digital Health Strategy for South Africa, 2019-2024', https://knowledgehub.health.gov.za/elibrary/national-digital-health-strategy-south-africa-2019-2024#:~:text=The%20new%20strategy%20sets%20out,life%20for%20all%20South%20Africans'.

[11] Ibid, p. 11

persisting digital health challenges in South Africa as fragmented systems, poor return on investments, budget constraints, skills shortages, inadequate infrastructure, and unaffordable broadband costs. It notes that previous laws like the National Health Act, the Electronic Communications Act, and the Protection of Personal Information Act have provided a strong legal basis but require additional updated regulations tuned to emerging technologies.

By establishing local digital health leadership structures, undertaking multi-stakeholder participation, securing dedicated digital health investments potentially through innovative financing, enabling national interoperability, developing user-centric applications like the health record and health apps store, addressing network infrastructure deficiencies, and boosting technical expertise, the new strategy underscores political will and systematically seeks to foster digital health adoption in South Africa to transform service delivery.

In addition to the strategy, there is also the **2021 Health Normative Standards Framework (HNSF) for Digital Health Interoperability in South Africa** which provides standards to enable different digital health systems like electronic medical records, mHealth apps and wearables to exchange data and operate seamlessly and securely across the health ecosystem.[12] As outlined under the National Health Act's Section 74, the HNSF ensures syntactic, semantic and technical interoperability through common terminology, coding schemas and exchange protocols. This permits accessible, meaningful and trusted health information flows between patients, providers and health authorities. The HNSF steers the approach for assuring security, privacy and interoperability in digital health implementations. It serves as an additional instrument supplementing legal provisions to ensure patient safety, system integration and responsible data usage within the evolving South African digital health landscape.

The legal and regulatory landscape in South Africa, as delineated by the Constitution, the National Health Act, the Health Professions Act, the Protection of Personal Information (PoPI) Act, the Electronic Communications and Transactions (ECT) Act, the Promotion of Access to Information Act, the Consumer Protection Act, and the Medicines and Related Substances Act, provides a multifaceted framework that indirectly supports and governs aspects of digital health. However, the rapid proliferation of health apps and digital health technologies raises questions about the existence of regulatory vacuums, particularly in areas like cybersecurity, data privacy, and the oversight of health apps that handle sensitive information. These existing laws collectively contribute to a foundation for regulating digital health, emphasising patient rights, data protection, and the ethical use of digital technologies in healthcare. Yet, the nuanced challenges posed by digital health—such as the integration of foreign apps, the complexity of cybersecurity threats, and the intricacies of handling sensitive health data in a digital ecosystem—suggest that there might be conspicuous gaps in the regulatory framework.

The absence of a specific Act that directly addresses threats and penalises misconduct in the digital health space is indicative of such a gap. While the PoPI Act provides principles for data protection and privacy, the enforcement mechanisms and specific regulations tailored to the unique vulnerabilities of the health sector may not be sufficiently robust to address the challenges. This is particularly relevant in the context of health apps, where sensitive patient information is at risk of breaches and unauthorised access. Furthermore, the regulation of foreign app providers operating outside the jurisdiction of South Africa introduces significant hurdles. The global nature of digital health services, coupled with the reliance on third-party agreements that underpin app functionality, necessitates a regulatory framework that extends beyond national borders. This includes mechanisms for international cooperation and data governance agreements that ensure foreign providers comply with South African laws, such as PoPI. However, the effectiveness of PoPI's reach in this international context remains untested, posing potential risks to patient privacy and data security.

[12] Republic of South Africa, Department of Health, '2021 Health Normative Standards Framework, 2021', https://www.health.gov.za/wp-content/uploads/2022/10/HNSF_Gazette_21_October_2022.pdf

The oversight of health apps, especially those handling sensitive information, requires stringent regulatory measures that are currently not explicitly outlined in the existing laws. While the Consumer Protection Act and the Medicines and Related Substances Act provide some degree of oversight, particularly in terms of false claims and the regulation of medical devices, there is a need for more detailed regulations that address the specific challenges of digital health technologies. This includes standards for app efficacy, safety, privacy, and interoperability.

2.1.2. Governing Institutions

Building on the legislative and regulatory analysis, it is also pertinent to critically examine the institutional governance landscape involved in overseeing South Africa's digital health ecosystem. A range of government bodies, specialised agencies and statutory structures with differentiated mandates span critical oversight functions across the domains of health policies, standards setting, service delivery models, health technologies, data governance and ethical practice regarding digital health adoption.

The **National Department of Health**,[13] as steward of the health system, has overarching duties under Chapter 1 of the National Health Act to set national eHealth policies and guidelines for establishing the national health information system across public and private healthcare providers. This enables the Department to coordinate digital systems implementation. The **Office of Health Standards Compliance**[14] instituted through Sections 77-79 of the Act certifies and enforces quality standards at health establishments providing telemedicine services and implementing hospital management health information systems. By conducting normative inspections, the OHSC provides additional oversight for digital health alongside the health department. The **Health Professions Council of South Africa (HPCSA)**,[15] established under the Health Professions Act as the statutory body coordinating the medical profession, plays a vital role in regulating telemedicine service delivery models, mHealth apps providing clinical diagnosis/treatment and ethical conduct of practitioners regarding patient privacy/consent when adopting digital health platforms through its ethical rules and guidelines.

The HPCSA has formulated guidelines around clinical usage of messaging apps including WhatsApp to check the power asymmetries that can emerge from private sector dominance over enabling infrastructure without commensurate accountability.[16] Despite lacking some security and consent safeguards for health data exchanges, WhatsApp's convenience, reach and usability has seen extensive usage for clinician communications, teleconsultations and patient record transfers. However, this dependence concentrates control with private systems like Facebook-owned WhatsApp lacking robust guarantees around commercial usage, third party sharing or location of stored data. In this vein Bouter et al[17] explain that the HPCSA guidelines hence recognise WhatsApp's clinical utility but recommend physicians limit usage to basic health purposes, retain consent records and not rely solely on unapproved systems lacking requisite security, uptime or stability necessary for ethical telemedicine. It reflects governments seeking to balance innovation incentives and public safeguards through soft policy guidelines where regulations lag private innovation.

In addition, Section 75 of the National Health Act empowers the Minister to institute **committees** to advise on standards for health technologies and information systems. This has seen the

[13] National Department of Health, https://www.health.gov.za/

[14] Office of Health Standards Compliance, https://ohsc.org.za/

[15] Health Professions Council of South Africa (HPCSA), https://www.hpcsa.co.za/

[16] Health Professions Council of South Africa. Ethical guidelines on social media. 2019. https://www.hpcsa.co.za/Uploads/Events/Conference/20Aug_Session_4_Guidelines_for_Social_Media.pdf

[17] Bouter C, Venter B and Etheredge H, 'Guidelines for the use of WhatsApp groups in clinical settings in South Africa', *S Afr Med J* 2020;110(5):364-368.

emergence of the **National Health Information Systems of South Africa Committee (NHISSA)**[18] that support interoperability, terminology standards, enterprise architecture, and health data exchange across digital systems. Furthermore, **the South African Health Products Regulatory Authority (SAHPRA),**[19] set up through the Medicines and Related Substances Act, serves as the medical device regulator providing approval based on safety, quality and efficacy related to clinical claims and performance made by mobile medical applications, eHealth systems and telemedicine technologies. Moreover, the **Information Regulator**[20] created under the Protection of Personal Information Act governs responsible and lawful processing, sharing and security of patients' health data by public/private sector digital solutions dealing with personal information to assure confidentiality and privacy.

The **Ministry of Communications and Digital Technologies**[21] is responsible for overseeing policies, laws and regulations pertaining to the information and communications technology (ICT) sector infrastructure and services spanning telecoms, broadband, internet, electronics and data governance. Since digital health solutions extensively utilise ICT platforms for enabling innovations in electronic health records, telemedicine provision, mHealth apps, remote patient monitoring and health data exchange, the Ministry plays an instrumental role regarding connectivity infrastructure and data costs impacting affordability and reliability of health technologies. The Ministry's leadership is essential concerning optimal policy harmonisation across healthcare priorities and national ICT development goals enabling South Africa's digital transformation.

The **Independent Communications Authority of South Africa (ICASA)**[22] is the regulatory body empowered under the Electronic Communications Act for licensing and regulating broadcasting and electronic communications platforms. Since digital health solutions increasingly utilise mobile, internet and telecommunications infrastructure for enabling remote care, patient monitoring and mHealth innovations, ICASA plays a pivotal role in governing aspects like spectrum allocation, service costs and universal access obligations that impact connectivity for digital health. Initiatives undertaken by ICASA like reducing data costs thus indirectly influence the accessibility, affordability and interoperability of health technologies relying on stable, high-speed networks and communications channels. Through its policy and regulatory purview over the ICT sector, ICASA therefore constitutes another important governance institution along with the health and medical counterparts regulating usage, data, technologies and ethics regarding the adoption of digital health platforms in South Africa.

Finally, the **South African Medical Association (SAMA)**[23] serves as the largest professional association representing medical practitioners in the country. Under its constitutional objectives, SAMA assists providers in upholding ethical standards concerning technologies like telemedicine and mHealth apps that are transforming healthcare delivery models. Through issuing ethical guidelines, position statements, continuing education and advocacy regarding clinical usage of digital health platforms, SAMA constitutes physicians' collective voice providing peer oversight for appropriateness, privacy protections and mitigating medicolegal risks associated with embracing new health technologies alongside statutory bodies like the HPCSA.

These governing institutions reflect a complex, cross-cutting regulatory landscape spanning domains from health policies, medical ethics, service delivery platforms, connectivity infrastructure and data governance. While having differentiated oversight mandates allows concentrated focus, the involvement of the Department of Health, SAHPRA, HPCSA, Information Regulator, ICASA, Ministry of Communications, NHISSA across digital health results in a somewhat fragmented rather than

[18] https://www.health.gov.za/wp-content/uploads/2020/11/national-digital-strategy-for-south-africa-2019-2024-b.pdf
[19] South African Health Products Regulatory Authority (SAHPRA), https://www.sahpra.org.za/
[20] Information Regulator, https://inforegulator.org.za/
[21] Ministry of Communications and Digital Technologies, https://www.dcdt.gov.za/
[22] Independent Communications Authority of South Africa, https://www.icasa.org.za/
[23] South African Medical Association, https://www.samedical.org/

coherent singular governance architecture. This fragmentation breeds potential risks of regulatory gaps or duplication. For instance, health apps could fall under simultaneous scrutiny regarding clinical standards from SAHPRA and HPCSA, while facing data privacy reviews by the Information Regulator as well as quality of service investigations by ICASA if leveraging telecommunications channels. Navigating this overlapping web of regulators imposes compliance burdens and uncertainty for digital health innovators.

It also impedes regulators from taking wholesome accountability for digital health growth as specific aspects like ethical practice, interoperability norms or cybersecurity may lack integrated oversight. Implementation could suffer too if institutional coordination on shared priorities is inadequate despite individual functioning. Moreover, the acts empowering the various authorities like NHISSA, HPCSA or OHSC were enacted before the ascent of digital health terminologies thereby lacking updated provisions for emerging technologies. Regulatory reforms to address fragmentation through harmonisation mechanisms between institutions combined with legislation updates are hence imperative. Nonetheless, the multiple centres of expertise within government reflect institutional foundations to build upon through improved cooperation. Bodies like SAMA also signify engaged medical community stakeholders while consumer protection forums safeguard patient interests.

These views are also expressed by Barit[24] who has analysed South Africa's institutional framework, and his analysis posits that the institutional landscape in South Africa appears constrained in effectively regulating various facets of digital health such as health apps and telemedicine models due to restrictive professional guidelines that have not kept pace with technological advancements. The HPCSA, he argues has a narrowly defined scope for what constitutes permissible telemedicine through its ethical rules framed prior to the digital health epoch. By requiring in-person physical consultations between providers and patients as a prerequisite for diagnosis, treatment or issuing prescriptions, the HPCSA effectively prohibits virtual care models like symptom checkers, automated prescription renewals via apps, online doctor consultations or remote monitoring.

As Barit highlights through the failed case of Hello Doctor and examples of video-enabled pharmacy dispensing units, such outdated guidelines are at odds with innovative attempts to increase healthcare access, efficiency and affordability leveraging technologies. They also clash with public sector initiatives like MomConnect that utilise digital platforms for maternal health awareness and two-way engagement. Barit argues that the disproportionate gatekeeping through ethical codes crafted before the ascent of handheld devices, wearables and mobile apps combined with a lack of research on risks in the local context regarding remote care restrict the regulatory space for dynamically responding to technology-enabled care models. It limits the evaluation of solutions that could alleviate access barriers for rural, elderly or disabled populations; reduce needless healthcare expenditure and waiting times; or enhance patient education and self-care.

Fundamentally, Barit cautions that there is a need to recalibrate the institutional regulatory mindsets from physical-first care paradigms to patient-centric, technology-leveraged paradigms to craft appropriate governance scaffolding that aligns South Africa's health system with the Fourth Industrial Revolution's dynamism. The failure by these existing institutions to bridge this emerging lacuna risks widening access gaps or fostering regulatory workarounds detached from systemic oversight. Chuma and Sibiya's[25] analysis of fragmentation in South Africa's health system further highlights the institutional fragmentation that impedes effective governance. They note how healthcare delivery spans national, provincial, and local government bodies like municipalities with facilities falling under decentralised administrative control. This dispersed accountability across multiple layers of entities operating independently fosters disconnects in healthcare provision.

[24] Barit A, 'The apps are coming! But will they be legal in South Africa?', *S Afr Med J* 2019; 109(3):150-151.

[25] Chuma K and Sibiya P., 'Digital Health Ecosystem Framework to Address Fragmentation of the Health System in South Africa', *Africa Journal of Nursing and Midwifery*, Vol 24, No. 2 (2022).

For instance, policies, priorities, and digitisation efforts regarding clinics in a district could diverge from provincial priorities. With South Africa's public health system separating into primary, district and tertiary services, such fragmented governance based on the tier of care further exacerbates coordination problems. Chuma and Sibiya surface how this fragmentation permeates into the usage of disparate, unconnected health information systems implemented in siloed fashion without enterprise-wide cohesion. This systemic fragmentation in institutional oversight, compounded by the bifurcation between digitised private healthcare and public sector facilities, entrenches data siloes and continuity of care gaps for patients navigating complex transitions. It elucidates why previous eHealth policies like the national eHealth strategy have fallen short of resolving such entrenched fragmentation.

While governmental bodies have provided some oversight policies, the digital health landscape also involves a complex array of private entities, non-profit groups, startups and global collaborators participating actively in advancing digital health through apps, often in siloed initiatives. There is certainly innovation happening, for example how Vula Mobile's app[26] links public facilities and patients.[27] However, such mobile health advancements seem to still occur in pockets within overall systemic fragmentation, rather than through coordinated governance or enterprise-level roadmaps. As Kapepo et al.[28] analysis of the Vula mobile health application suggests, such mobile health innovations continue to perpetuate fragmentation rather than contribute to coordinated systems integration. They note persisting challenges like problematic self-referrals indicating continued lack of health systems integration, widespread use of informal tools like WhatsApp groups signalling data siloes, on-ground adoption constraints versus national interoperability visions, and workaround practices fitting immediate needs rather than managing change through enterprise initiatives.

Thus, while discrete mHealth deployments like Vula application showcase pockets of innovation, overcoming the bifurcation between national policies and ground realities requires progressing from such fragmentation towards synchronised governance and implementation frameworks that align standards and stakeholders. Bridging this disconnect is imperative for systemic advancement rather than isolated innovation success. It is therefore important to understand who the other actors are in the digital health space in South Africa.

2.1.3. Actors

Beyond governmental bodies, South Africa's digital health ecosystem involves an array of non-state actors spanning philanthropies, private tech providers, insurers, entrepreneurs and foreign collaborators that steer various aspects with or without regulatory guidance. For instance, the Rockefeller Foundation has supported the established MomConnect platform leveraging their technical expertise in scaling mobile innovations.[29] The Praekelt Foundation served as lead technical implementer of MomConnect demonstrating local philanthropy's convening capacity to catalyse public-private partnerships on shared health priorities.[30]

Praekelt, a homegrown non-profit, served as the original developer and implementing partner for the MomConnect maternal health messaging system since its pilot days as part of the MAMA initiative supported by global donors. When South Africa's National Department of Health sought to

[26] https://www.vulamobile.com/

[27] Steyn L., Mash RJ and Hendricks G., 'Use of the Vula App to refer patients in the West Coast District: A descriptive exploratory study', *S Afr Fam Pract* (2022) 64:(1): 5491.

[28] Kapepo MI., van Belle JP and Weimann E., 'Towards a theoretical understanding of workarounds emerging from use of a referral mobile application: a developing country context'*, Procedia Computer Science 196* (2022) 533-541.

[29] The Rockefeller Foundation, 'The Rockefeller Foundation Commits Nearly USD 35 Million to Covid19 Response Efforts in Africa', Press Release, Feb 03, 2021, https://www.rockefellerfoundation.org/news/the-rockefeller-foundation-commits-nearly-usd-35-million-to-covid-19-response-efforts-in-africa/

[30] Digital Impact Alliance, MomConnect, Praekelt Foundation, South Africa, http://im.digitalimpactalliance.org/MomConnect.html

transition such mobile innovation to national scale as an official state program, Praekelt's technical capacity and localisation knowledge enabled a smooth public handover establishing MomConnect's expansive reach across provinces.[31] This demonstrates the convening ability of social impact-driven private players to align innovations with public health imperatives, shifting from isolated pilots to standardised platforms reaching underserved communities nationwide. Furthermore, to maximise access, MomConnect also integrated popular social messaging apps like WhatsApp through bespoke early-adopter APIs to provide richer user engagement, showcasing adaptiveness to leverage private advancements suiting local contexts.[32] This may also have posed risks regarding data privacy from MomConnect's integration with WhatsApp.

As Reichel et al[33] highlight, WhatsApp's end-to-end encryption comes at the cost of requiring in-house infrastructure that smaller developers may struggle to implement securely. Additionally, WhatsApp's parent Facebook has been known to mine user data for advertising purposes from its products like Messenger. Hence the MomConnect-WhatsApp integration may have inadvertently exposed sensitive maternal health data of users to third-party tracking for commercial interests without sufficient safeguards. While Praekelt claimed to have appropriate data security measures,[34] the technological complexity leaves open the possibility of confidentiality breaches, however inadvertent. This could violate users' autonomy and the right to consent regarding use of their personal health information. The platform integration likely prioritised rapid reach of MomConnect's health messaging over evaluating risks like third-party data sharing inherent in proprietary systems like WhatsApp. Thus, according to Obuaku-Igwe[35] efficiency for scale may have taken precedence over assuring ethical compliance. The initial excitement over expanding access eclipsed considerations of how dependence on foreign systems with embedded commercial prerogatives might entangle public interest commitments to equity and privacy.

Local startups like HealthEnabled[36] and global tech giants like Google provide proprietary APIs that the National Health Department utilises for screening, diagnostics and patient monitoring applications. Their footing as private innovators allows them latitude to advance digital capabilities even where policy lags, while state ties and health sector knowledge allow alignment with public objectives. These non-state actors often hold proprietary control over platforms processing sensitive health data. As Tiffin et al[37] caution, such private interests oriented towards efficiency, scale and profits can undermine adequate safeguards for equitable, ethical usage of data from marginalised communities. They explain that significant reliance on external players for core health messaging and diagnostics infrastructure concentrates control over personal health data with private systems lacking accountability. For instance, MomConnect's dependency on WhatsApp servers for expanded reach risks exposing maternal health records to third-party mining given Facebook's track record on commercial usage despite stated privacy protections.

Tiffin et al also point out that non state actor involvement in digital health enable foreign commercial entities to influence policies around healthcare data sharing, access and transparency based on their technological dominance thereby disempowering local health institutions from securing citizen

[31] Ibid.
[32] Ibid.
[33] Reichel J., Peck F., Inaba M, et al., 'I have too much respect for my elders: understanding South African Mobile Users Perceptions of Privacy and Current Behaviours on Facebook and WhatsApp', 29th USENIX Security Symposium, August 12-14, 2020, https://www.usenix.org/conference/usenixsecurity20/presentation/reichel
[34] Digital Impact Alliance, MomConnect, Praekelt Foundation, South Africa, http://im.digitalimpactalliance.org/MomConnect.html
[35] Obuaku-Igwe C., 'The Effectiveness of E-Health Services: Evidence from MomConnect in South Africa' *Academia Letters*, Article 577 (2021).
[36] HealthEnabled, https://healthenabled.org/
[37] Tiffin N, George A and LeFevre AE., 'How to use relevant data for maximal benefit with minimal risk: digital health data governance to protect vulnerable populations in low- income and middle-income countries', *BMJ Glob Health* 2019;4:e001395.

privacy.[38] They also open backdoors for misuse in contexts with limited regulatory oversight like inadequate enforcement of consent requirements or data localisation laws. Bouter et al[39] studying the pitfalls on the use of WhatsApp by healthcare professionals have further pointed out that reliance on proprietary software, algorithms and terms of service of private actors in the digital health space decouples decision making around appropriate health data usage from public interest priorities around ethics, equity and social justice that constitutionally inform South Africa's health rights framework.

Thus, while such private collaborations enable agility, resources and expertise facilitating effective digitisation, considerations around underlying motives, accountability, transparency and community participation warrant proactive governance interventions to check threats to privacy and autonomy, guard against exclusion and ensure truly empowering impacts on population health. Relatedly, Toebes[40] has argued that failing to centre human rights risks private efficiencies subverting public safeguards.

South Africa also has emerging private insurance players like Momentum[41] jumping into virtual medical care in partnerships with providers like Hello Doctor[42] telemedicine to steady clinical oversight. While guided by statutes like the Medical Schemes Act[43] and aligned ethical rules, their digital health forays occur at pace with regulation. However, market competition rather than national stewardship, argue Gumede and Manenzhe[44] often dictates their technology innovation and service differentiation strategies. Foreign collaborations tap global expertise for localised challenges. But Donnelly[45] has argued that balancing commercial gains against public health gains pose ongoing coordination complexities between multinational and state priorities within these cross-border partnerships.

Building on the analysis of state and non-state roles, the increasing infiltration of private interests in digital health also risks enabling creeping commercialisation counter to rights-based imperatives as per Toebes'[46] cautionary argument. The technical efficacy and scalability benefits private entities bring must be balanced with reasonable safeguards against proprietary data control, profit maximisation superseding public interest and lack of transparency in usage terms that violate rights to dignity, autonomy and privacy. For instance, private platform ownership of health data trails like MomConnect, lack of oversight into closed algorithms shaping diagnostics tests or screening results from Google/Apple APIs and unilateral control over such personal health information concentrate significant power with private players, often foreign multinationals. As much as such technical interventions fill crucial health system gaps, unchecked commercial prerogatives raise the possibility of entrenching health disparities, inequities and uneven access in ways that further undermine South Africa's constitutional right to healthcare instead of progressively enabling it.

[38] Ibid.

[39] Bouter C, Venter B and Etheredge H, 'Guidelines for the use of WhatsApp groups in clinical settings in South Africa', *S Afr Med J* 2020;110(5):364-368.

[40] Toebes, B., 'Taking a Human Rights Approach to Healthcare Commercialization', in Toebes, B (ed) *Health Capital and Sustainable Socioeconomic Development* (Routledge, 2008).

[41] https://www.momentum.co.za/momentum/home

[42] Momentum, "Momentum still offers Hello Doctor service for COVID-19 and other client requirement', 16 July 2020, https://www.momentum.co.za/momentum/media-centre/16-july-2020

[43] Republic of South Africa, 'Medical Schemes Act no 131 of 1998', https://www.gov.za/documents/medical-schemes-act

[44] Gumede S and Manenzhe P., "Competition regulation for digital markets: The South African Experience', *The African Journal of Information and Communication*, No. 31 (2023).

[45] Donnelly D., 'First Do No Harm: Legal Principles Regulating the Future of Artificial Intelligence in Health Care in South Africa', *PER / PELJ* 2022(25)

[46] Toebes, B., 'Taking a Human Rights Approach to Healthcare Commercialization', in Toebes, B (ed) *Health Capital and Sustainable Socioeconomic Development* (Routledge, 2008).

Unchecked private interests in leveraging health data for profits can undermine digital health's public interest mandate, as Botes et al[47] have cautioned. These authors argue that private actors like insurers or commercial diagnostic firms in South Africa accumulating expansive health data troves and opaque algorithms for commercial gains absent binding accountability on equity or non-discrimination makes the ecosystem's human rights commitments vulnerable. For instance, insurance spin-offs gaining hereditary insight from genomic tests to determine premiums based on predictive lifetime disease risk unfairly disadvantages families with congenital conditions despite Constitutional protections. Similarly, biobanks sharing samples internationally for micro-array development signify misaligned profit incentives limiting consent, oversight or benefit-sharing with sample sources.[48]

2.1.4. Testing Environment for Health Apps

The emergence of mobile health apps has introduced a new paradigm in South Africa's healthcare landscape, prompting discussions about the adequacy of the existing regulatory framework to ensure user safety, privacy, and legal compliance. While the country's legislative and policy environment, as outlined in the National Digital Health Strategy 2019-2024[49] and the Health Normative Standards Framework for Interoperability in eHealth in South Africa[50] recognises the potential of digital health solutions to enhance accessibility, efficiency, and quality of care, questions remain about the robustness of the testing environment for health apps prior to their public deployment.

A critical examination of South Africa's regulatory landscape reveals the absence of a clear mandate for controlled testing of health apps to identify and mitigate risks to user safety and privacy. The Protection of Personal Information Act 4 of 2013 (POPIA)[51] which governs the processing of personal information, including health data, provides a foundation for data protection principles such as lawful processing, purpose specification, and security safeguards. However, the Act's effectiveness in ensuring meaningful consent and enforcing compliance remains limited, particularly in the context of health apps developed by foreign entities operating outside South Africa's jurisdiction.

The regulatory sandbox concept, which has gained traction in the financial technology (fintech) sector, offers a potential avenue for controlled testing of health apps. Regulatory sandboxes provide a controlled environment for innovators to test new products and services under the oversight of regulators, allowing for the identification of risks and the development of appropriate regulatory responses.[52] In South Africa, the Intergovernmental Fintech Working Group (IFWG) has established a regulatory sandbox focused on fintech innovations, with a particular emphasis on crypto assets, cross-border payments, and crowdfunding.[53] However, the absence of a similar initiative in the digital health space highlights a regulatory gap. The current fintech-focused regulatory sandbox does not cater to the unique challenges posed by health apps, such as the sensitivity of health data, the potential for misdiagnosis or improper treatment, and the ethical considerations surrounding the use of artificial intelligence and machine learning algorithms in healthcare decision-making.

Moreover, while POPIA provides a legal framework for data protection, its enforcement reach remains restricted, particularly in the context of health apps developed and operated by foreign entities. The

[47] Botes M, Olckers A and Labuschaigne M., 'Data Commercialisation in the South African Health Care Context', *PER / PELJ* 2021(24).
[48] Ibid., p.11-20.
[49] Supra, n10
[50] Supra, n12
[51] Supra, n5
[52] Ross P Buckley and others, 'Building FinTech Ecosystems: Regulatory Sandboxes, Innovation Hubs and Beyond' (2019) European Banking Institute Working Paper Series 53.
[53] Intergovernmental Fintech Working Group, 'Feedback on the Intergovernmental Fintech Working Group's first regulatory sandbox initiative' (12 October 2022).

extra-territorial application of POPIA to foreign entities processing personal information of South African citizens is limited by practical constraints in investigating and prosecuting non-compliant entities outside the country's jurisdiction.[54] This regulatory gap leaves South African users of foreign health apps vulnerable to potential data breaches, unauthorised sharing of sensitive health information, and exploitation for commercial purposes. The lack of a dedicated testing environment for health apps also raises concerns about the adequacy of consent mechanisms and transparency in data processing practices. Health app developers may not fully disclose the extent of data collection, the purposes for which the data will be used, or the third parties with whom the data may be shared. Without a controlled testing environment to scrutinise these practices and ensure compliance with POPIA's consent and processing requirements, there is a risk of users unwittingly sharing their sensitive health information without fully understanding the implications.

While South Africa's legislative and policy framework recognises the potential of digital health technologies, the absence of a clear mandate for controlled testing of health apps prior to public deployment represents a significant regulatory gap. The current fintech-focused regulatory sandbox does not address the unique challenges posed by health apps, leaving users vulnerable to potential risks to their safety and privacy. The limited enforcement reach of POPIA, particularly in the context of foreign entities, further underscores the need for a dedicated testing environment to ensure compliance with data protection principles and meaningful consent mechanisms.

2.1.5. Lessons Learned

The regulatory framework for digital health in South Africa is characterised by fragmentation, creating uncertainties and potential accountability gaps. The involvement of multiple regulatory bodies, each with differentiated oversight mandates, such as the Department of Health, SAHPRA, HPCSA, Information Regulator, and ICASA, results in a complex and potentially overlapping web of regulators. This fragmentation breeds potential risks of regulatory gaps or duplication, imposing compliance burdens and uncertainty for digital health innovators. Furthermore, the existing acts empowering various authorities, such as the National Health Act and the Health Professions Act, were enacted before the ascent of digital health terminologies, lacking updated provisions for emerging technologies. Several further knowledge gaps are revealed:

Firstly, while South Africa has made notable progress in adopting digital health technologies to expand healthcare access and improve efficiency, there is limited research on the actual efficacy, quality, and safety of specific health apps and digital platforms within the South African context. This knowledge gap hinders the ability of policymakers and regulators to make informed decisions and develop targeted interventions to ensure that these technologies are delivering the intended benefits while minimising potential risks to users. This is evidenced from the National Digital Health Strategy for South Africa 2019-2024 and the 2021 Health Normative Standards Framework (HNSF) for Digital Health Interoperability in South Africa that do not make provisions on health apps in terms of their regulation.

Secondly, the perspectives and experiences of consumers engaging with digital health technologies in South Africa remain largely unexplored. As health apps and platforms increasingly rely on accessing and processing intimate personal data, it is crucial to understand how users across different socioeconomic and literacy levels comprehend and navigate complex consent mechanisms and data-sharing agreements. Investigating the sociocultural factors that influence user understanding and agency in the face of algorithmic decision-making and evolving backend architectures is essential for developing inclusive and protective regulatory frameworks.

Thirdly, although South Africa has made strides in developing policies and strategies related to digital health, there are still significant gaps in the accountability mechanisms governing the complex data

[54] Anneliese Roos, 'Data protection in South Africa: The Protection of Personal Information Act and the right to privacy' (2021) 54 *The International Journal of Intelligence, Security, and Public Affairs* 235.

flows between patients, third-party suppliers, platform owners, and the state. The existing regulatory landscape appears fragmented and lacks the necessary scaffolding to enforce comprehensive standards across the diverse array of apps, devices, and systems that collectively impact healthcare access and outcomes. Strengthening the practical capacity for continuous monitoring and swift intervention in the face of rapidly evolving digital health architectures remains a critical challenge.

Fourthly, there is a need for evidence-based research that traces specific instances of personal health data exploitation, privacy infringements, and surveillance risks in the South African context. Documenting empirical cases where algorithmic inferences or third-party partnerships have compromised patient welfare or led to discriminatory outcomes is crucial for assessing the efficacy of existing regulations and catalysing necessary policy reforms. Similarly, identifying instances where a lack of interoperability or data portability has hindered user agency and perpetuated data silos is essential for promoting a more patient-centric digital health ecosystem.

Fifthly, the accelerating convergence of public and private interests in the mediation of healthcare access through digital technologies warrants closer examination in South Africa. As health apps and digitised financing mechanisms become more pervasive, the implications for the state's obligation to respect, protect, and fulfil the fundamental right to health must be carefully analysed. The commercialisation of digital health services raises concerns about potential conflicts between profit motives and public health priorities, as well as the limitations of human rights law in holding private actors accountable for delegated responsibilities.

In addition to these knowledge gaps, there is a pressing need for conceptual clarity around key terms and principles that underpin the regulation of digital health in South Africa. Notably, the notion of meaningful consent, which is central to data protection and patient autonomy, requires further elucidation. As users are often confronted with lengthy and opaque terms of service agreements, the boundaries of informed and voluntary participation become blurred. Similarly, the concepts of interoperability and data portability need to be more explicitly defined and enshrined within policy frameworks to prevent vendor lock-in and empower patients to exercise greater control over their health information. The meaning and scope of data protection itself should be expanded to encompass not only protection against unauthorised appropriation but also safeguards against the continual referencing and updating of personal data by self-learning algorithms.

Lastly, the analysis of South Africa's digital health landscape reveals several areas that require legal reform and regulatory innovation. While existing legislation, such as the National Health Act, the Protection of Personal Information Act (POPIA), and the Electronic Communications and Transactions Act, provide a foundational framework for governing digital health, they may not adequately address the unique challenges posed by health apps and algorithmic decision-making. Updating these laws to specifically cover the complexities of digital health technologies and establishing dedicated oversight mechanisms for the entire digital health ecosystem, including software vendors, data processors, and AI providers, is crucial for ensuring a coherent and effective regulatory environment.

Moreover, the absence of a clear regulatory sandbox or controlled testing environment for health apps in South Africa represents a significant gap that needs to be addressed. Establishing such a sandbox, similar to the fintech-focused initiative by the Intergovernmental Fintech Working Group (IFWG), would provide a safe space for innovators and regulators to collaborate, assess risks and benefits, and develop evidence-based guidelines for the responsible development and deployment of health apps.

2.2. The Health Apps Ecosystem

2.2.1. Methods

In studying the health app ecosystem in South Africa, purposive sampling was employed to select a representative set of health apps popular within the South African context. This sampling method was chosen to ensure the inclusion of apps with significant presence and impact in South Africa's digital health ecosystem. The selection was based on the visibility of apps in web and newspaper articles and mentions within academic literature. Both locally developed apps and foreign-developed apps marketed in South Africa were included.

Specifically, the study focuses on Kena Health[55], a locally developed app by Cardo Health[56], a foreign startup. Kena Health was chosen due to its recognition as a locally developed app and its potential impact on the South African healthcare landscape. Additionally, MomConnect[57], a locally developed maternal health app, was selected for its widespread use and impact on maternal and child health in South Africa. MomConnect has been widely recognised for its innovative approach to supporting pregnant women and new mothers through mobile technology. To provide a comparative perspective, a foreign-developed app, Ada, was also considered due to its marketing efforts in the country and the availability of online information about its operation and use in South Africa. Ada is a globally recognised health app that uses artificial intelligence to help users assess their symptoms and provide guidance on potential health issues.

A detailed analysis of the terms and privacy policies of these three apps - Kena Health, MomConnect, and Ada - was conducted to identify legal nuances and potential implications for user privacy and data protection. The analysis aimed to uncover any similarities, differences, or potential gaps in the way these apps handle user data and comply with South African legal and regulatory frameworks. By comparing the terms and privacy policies of a locally developed app (Kena Health), a government-supported maternal health app (MomConnect), and a foreign-developed app marketed in South Africa (Ada)[58], the study seeks to provide a comprehensive understanding of the legal landscape surrounding health apps in the country. This analysis will contribute to the broader discussion on the challenges and opportunities presented by the growing health app ecosystem in South Africa, and the potential lessons that can be learned from the terms and privacy policies of these specific apps.

2.2.2. Overview of the Digital Health Ecosystem

Serbanati et al[59] describe the digital health ecosystem as a dynamic and interdependent environment, where various 'digital species' – such as healthcare providers, institutions, technologies, and regulatory frameworks – coexist and interact. They conceptualise it as 'a network of a multitude of agents: care providers (physicians, nurses, pharmacists, and other health professionals), health suppliers, together with their organisations and information systems, care consumers, plus the socio-economic environment and including the health institutional and regulatory framework'. This ecosystem is envisioned as a collaborative space that fosters cooperation, knowledge sharing, and the development of open and adaptive technologies. Within this broader ecosystem, the landscape of health apps emerges as a distinct yet intricately connected domain.

The digital health ecosystem in South Africa is a complex and evolving landscape, shaped by a multitude of factors including legislative frameworks, regulatory bodies, technological advancements, and societal needs. It paints a picture of a complex and intricate digital health ecosystem in South Africa, characterised by an interconnected network of stakeholders spanning government, private entities, international collaborators, and various regulatory bodies. This ecosystem encompasses a diverse array of digital health interventions, including electronic health records, telemedicine platforms, mobile health applications (mHealth apps), and data exchange systems. The literature review conducted under this sub-section aims to explore the contributions of various scholars in understanding the current state

[55] https://www.kena.health/

[56] https://www.cardohealth.com/

[57] https://www.measureevaluation.org/sifsa/MomConnect.html

[58] https://ada.com/press/230905-ada-supporting-mothers-in-southafrica/

[59] Serbanati, L., Ricci, F., Mercurio, G et al., 'Steps towards a digital health ecosystem,' *Journal of Biomedical Informatics* 44:4 (2011) 621-636.

of South Africa's digital health ecosystem, with a particular focus on health apps and the regulatory environment surrounding them.

Herselman et al[60] provide a conceptual framework for a digital health innovation ecosystem in South Africa, highlighting the importance of context, the innovation lifecycle, and the involvement of various stakeholders. The authors emphasise the need for digital health solutions that are sensitive to local economic, social, cultural, and organisational factors, as well as the importance of a self-directed innovation ecosystem based on the common interests of all actors in a quadruple helix (government, industry, users or community, and universities). This framework serves as a foundation for understanding the complex interplay of factors that shape the digital health landscape in South Africa.

Ojo[61] offers a systematic review of the digital health ecosystem from the lens of mHealth interventions in South Africa, focusing on the effectiveness of these interventions in improving health outcomes. The review reveals that while mHealth holds great potential for enhancing healthcare access and quality, there is limited evidence to confirm the impact of mHealth interventions on improved health outcomes. Ojo highlights the need for more intervention studies to establish the effect of mHealth on health outcomes and healthcare delivery processes in the South African context.

Townsend et al[62] delve into the regulatory landscape of digital health by focusing on artificial intelligence (AI) in healthcare in Africa, with a specific focus on 12 selected countries, including South Africa. The authors identify the absence of sui generis AI regulation in these countries, but note recent developments in areas that inform AI adoption, such as digital health, data protection, consumer protection, and intellectual property. The study underscores the fragmentation of the African AI regulatory landscape and emphasises the importance of continued AI regulatory development to ensure that Africa is well-positioned for future AI adoption in health. In another study by Townsend et al[63], the authors explore the development of ethical guidelines for telemedicine in South Africa, addressing three distinct ethical issues: the fiduciary nature of healthcare and the changing nature of the doctor-patient relationship, privacy and confidentiality, and informed consent. The authors critique the Health Professions Council of South Africa's (HPCSA) telemedicine guidelines, identifying conceptual and operational difficulties within the existing framework. They propose a more nuanced and culturally sensitive approach to ethical guidelines, striking a balance between individual rights protection and transformative, ethical healthcare innovation.

These studies collectively highlight the multifaceted nature of South Africa's digital health ecosystem, encompassing technological, regulatory, ethical, and societal dimensions. While the potential for digital health technologies, including health apps, to improve healthcare access and outcomes is widely acknowledged, the authors consistently emphasise the need for context-specific solutions that address the unique challenges faced by the South African healthcare system.

One notable knowledge gap that emerges from the literature is the lack of comprehensive, evidence-based studies on the effectiveness of health apps and other digital health interventions in the South African context. Ojo's systematic review underscores this gap, calling for more intervention studies to establish the impact of mHealth on health outcomes and healthcare delivery processes. When discussing health apps, the authors focus on various aspects, including their potential to improve healthcare access, particularly in rural and underserved areas, as well as their role in enabling remote consultations and patient monitoring. However, they also highlight the regulatory and ethical challenges associated with

[60] Herselman M et al., 'A Digital Health Innovation Ecosystem for South Africa' (2016) IST-Africa 2016 Conference Proceedings.

[61] Ojo AI, 'mHealth Interventions in South Africa: A Review' (2018) 8 *SAGE Open* 1.

[62] Townsend BA et al, 'Mapping the Regulatory Landscape of AI in Healthcare in Africa' (2023) *Frontiers in Pharmacology*.

[63] Townsend BA, Scott RE and Mars M, 'The Development of Ethical Guidelines for Telemedicine in South Africa' (2019) 12(1) *South African Journal of Bioethics and Law* 19.

the use of health apps, such as data privacy, informed consent, and the changing nature of the doctor-patient relationship in the digital era.

In terms of the legal and normative landscape surrounding health apps in South Africa, Townsend et al.'s analysis of the AI regulatory environment reveals a fragmented approach, with no specific legislation addressing AI in healthcare.[64] However, the authors note that certain aspects of digital health, including health apps, are informed by existing legislation and regulatory frameworks, such as the National Health Act, the Protection of Personal Information Act (POPIA), and the HPCSA's telemedicine guidelines. Townsend et al.'s critique of the HPCSA's telemedicine guidelines highlights the need for a more nuanced and contextually relevant approach to ethical guidance in the digital health sphere.[65] The authors argue that the current guidelines fail to adequately address the complexities of telemedicine and the use of digital health technologies, such as health apps, in the South African context.

Further, Barit's[66] analysis of the legal and ethical implications of health apps in South Africa reveals a regulatory environment that is currently ill-equipped to address the unique challenges posed by these technologies. The author critiques the Health Professions Council of South Africa's (HPCSA) telemedicine guidelines, arguing that they are outdated and restrictive, potentially stifling lawful and ethical development of AI in healthcare. Barit emphasises the need for a more nuanced approach to regulation that balances individual rights protection with the need for innovative and transformative healthcare solutions, a sentiment echoed by Townsend et al. in their examination of the development of ethical guidelines for telemedicine in South Africa.[67]

Botes et al[68] provide a different analysis of South Africa's digital health ecosystem by delving deeper into the commercialisation of health data in South Africa, exploring the complex interplay between informed consent, data sharing, privacy, and confidentiality. The authors highlight the increasing value of health data in the context of the Fourth Industrial Revolution (4IR) and the potential for exploitation by various actors, including insurance companies and health researchers. They argue that while South Africa's legal framework, centred around the Protection of Personal Information Act (POPIA), provides a comprehensive and multi-layered approach to protecting personal information, gaps remain in terms of addressing the specific challenges posed by health data commercialisation and cross-border data sharing. Botes et al also highlight the importance of addressing algorithmic bias and fairness in the adoption of AI and health apps in South Africa. They note, unchecked commercial interests in the accumulation and use of sensitive health data can exacerbate existing health inequities and undermine the constitutional right to healthcare in South Africa. In this regard, Townsend et al[69] have also emphasised the need for regulators to proactively address the concerns of algorithmic bias and fairness, as AI systems have the potential to amplify and perpetuate patterns of systemic and structural social bias, particularly in relation to protected features like race and gender.

In terms of the specific focus on health apps, the literature reviewed provides insights into the current state of regulation and the challenges posed by these technologies in the South African context. Barit highlights the restrictive nature of the HPCSA's telemedicine guidelines, which effectively ban any consultation where the doctor is at a distance from the patient and only interacting via technology.[70] This stance is seen as a barrier to the adoption of health apps and telemedicine solutions that could potentially improve healthcare access and outcomes in underserved areas. Townsend et al argue that the HPCSA's guidelines should be more closely aligned with the provisions of the POPIA and emphasise

[64] Supra, n 62.

[65] Supra, n 63.

[66] Barit A, 'The Apps are Coming! But Will They Be Legal in South Africa?' (2019) 109(3) *South African Medical Journal* 150.

[67] Supra, n 63.

[68] Botes M, Olckers A and Labuschaigne M, 'Data Commercialisation in the South African Health Care Context' (2021) 24 *Potchefstroom Electronic Law Journal* 1.

[69] Supra, n 62.

[70] Supra, n 66.

the importance of obtaining informed consent in a manner that is culturally sensitive and accounts for the diversity of language and literacy levels in South Africa.[71] The literature also sheds light on the potential for health apps to be used for data collection and commercialisation purposes, raising concerns about privacy, informed consent, and the potential for exploitation. Botes et al. discuss the example of insurance companies using health apps and genetic testing to assess risk and potentially discriminate against individuals based on their health status or genetic predisposition to certain conditions.[72]

In terms of the norms being created around health apps in South Africa, the literature suggests a growing recognition of the need for a more adaptive and responsive regulatory framework that can balance innovation with patient safety and privacy. Townsend et al's call for a risk-based and rights-based approach to AI regulation in healthcare, incorporating principles of transparency, explainability, and accountability, represents an important step towards establishing norms for responsible innovation in the digital health space.[73] However, the literature also reveals significant knowledge gaps in terms of understanding the effectiveness of health apps and the impact of data commercialisation on health outcomes and equity in the South African context. Ojo's systematic review of mHealth interventions in South Africa highlights the need for more evidence-based studies to establish the impact of these technologies on health outcomes and healthcare delivery processes. Similarly, Botes et al. note the lack of comprehensive, evidence-based studies on the effectiveness of health apps and other digital health interventions in the South African context, underscoring the need for further research to inform policy and regulatory development.

South Africa has a burgeoning health app ecosystem, characterised by a proliferation of locally developed solutions as well as the adoption of foreign applications. For instance, the MomConnect platform[74], developed through a public-private partnership, leverages local expertise from the Praekelt Foundation while integrating popular messaging apps like WhatsApp to enhance user engagement. This integration, however, raises concerns about data privacy and the potential exposure of sensitive maternal health data to third-party commercial interests. The health app ecosystem in South Africa also demonstrates a complex interplay between locally developed solutions and the adoption of foreign apps. While locally developed apps like Vula Mobile[75] showcase pockets of innovation, their impact is often limited by systemic fragmentation and a lack of integration with broader health information systems. Conversely, the adoption of foreign apps, such as those from global tech giants like Google, introduces challenges related to data sovereignty, accountability, and the potential disempowerment of local health institutions.

Furthermore, native startups like Vula Mobile, Hello Doctor,[76] Pelebox[77] are ideating mobile health innovations tailored to local needs, indicating growing digital health entrepreneurship targeting accessibility gaps. However, dependence on foreign capital persists, with many local startups receiving external funding, limiting organic business model sustainability. Simultaneously, South Africa's smartphone diffusion enables user access to international health app repositories like iOS' App Store and Google Play. Adoption of foreign solutions like the German Ada app,[78] Kena Health[79] and various others listed on the app stores then occurs locally. This facilitates the transfer of effective health innovations across borders to benefit South Africans, either for free or paid. While exogenous apps could crowd out local competition, they can also inspire domestic innovation.

[71] Supra, n 63.
[72] Supra, n 68.
[73] Supra, n 62.
[74] https://www.health.gov.za/momconnect/
[75] https://www.vulamobile.com/
[76] https://www.hellodoctor.co.za/
[77] https://www.pelebox.com/
[78] https://ada.com/press/230905-ada-supporting-mothers-in-southafrica/
[79] https://www.kena.health/

The health app ecosystem in South Africa interconnects various categories of apps to provide integrated healthcare solutions. For instance, teleconsultation apps like Hello Doctor[80] facilitate patient-doctor video consultations, while Pelebox enables chat-based diagnosis and shares health information resources. On the patient data side, apps like Vula Mobile maintain digital health records and exchange information with electronic medical record systems. Health apps also integrate with payment platforms to enable services like insurance premium collection and cashless claims settlement. App linkages facilitate medicine delivery from e-pharmacies arising from e-prescriptions on apps. Public health apps like the COVID Alert SA App[81] tracing solutions feed into health ministry dashboards to direct response.

In terms of functionality, South African health apps are moving beyond merely providing health information to more complex functions like diagnosis, remote monitoring, care plan integration, financing schemes, and medicine delivery. Features encompass the entire patient journey from promoting preventive health to enabling provider access to supporting treatment. There is also a focus on providing holistic care spanning areas like wellness, disease management, and health needs. Regarding infrastructure, interoperability is emerging with national health insurance systems as well as private platforms. Data integration spanning patient records, pharmacy systems, and insurance claims is increasingly enabling continuity of care.

Taking all this into consideration, Tiffin et al[82] highlight the potential pitfalls of relying heavily on proprietary platforms and algorithms controlled by foreign commercial entities. The authors caution that such reliance can undermine adequate safeguards for equitable and ethical data usage, particularly in contexts where regulatory oversight is limited. Additionally, the integration of foreign apps may inadvertently enable backdoors for data misuse, compromising principles of informed consent and data localisation laws. The health app ecosystem in South Africa thus presents a microcosm of the broader digital health landscape, where the potential benefits of technological innovation are counterbalanced by concerns over data privacy, ethical oversight, and the intrusion of commercial interests that may subvert public health priorities.

2.2.3. Categorisation of Health Apps

Platforms such as SimilarWeb[83] and AppFigures[84] provide a window into the vast array of health apps available in South Africa. SimilarWeb lists around 50 apps under the ‘Medical’ category and another 50 under ‘Health & Fitness’ for South Africa. AppFigures lists around 200 free apps under ‘Medical’ and another 200 under ‘Health & Fitness’. However, these platforms do not offer the nuanced categorisation necessary to differentiate between apps developed locally or abroad, nor do they allow users to filter apps by their specific functions. This limitation points to the need for a more discerning approach in identifying and classifying health apps based on their origin and functionality in South Africa.

The discourse on health apps in the literature is characterised by a diversity of functional descriptors, each contributing uniquely to the understanding of these digital tools, yet without culminating in a standardised classification system. Neumark and Prince talk about ‘microinsurance apps’, ‘health wallets’ and ‘apps that support community health workers to order commodities’ directly, facilitating logistics and supply chain management in healthcare.[85] Erikson discusses the broader category of ‘mobile phone apps’, possibly encompassing a wide range of functionalities from patient engagement

[80] https://www.hellodoctor.co.za/

[81] https://www.discovery.co.za/corporate/download-covid-alert-sa-app-today

[82] Tiffin N, George A and LeFevre AE., ‘How to use relevant data for maximal benefit with minimal risk: digital health data governance to protect vulnerable populations in low- income and middle-income countries’, *BMJ Glob Health* 2019;4:e001395

[83] https://www.similarweb.com/top-apps/google/south-africa/medical/

[84] https://appfigures.com/top-apps/google-play/south-africa/medical

[85] Neumark, T and Prince, R.J., ‘Digital Health in East Africa: Innovation, Experimentation and the Market’ *Global Policy*, Vol 12, Supp 6 (2021).

to data capture.[86] Arueyingho and Sanyaolu bring attention to the surge in 'fitness mobile apps', highlighting the consumer-focused side of health apps that cater to personal wellness and activity tracking.[87] Lastly, Miller et al sheds light on 'smartphone apps' and the more targeted 'track and trace apps', which could refer to solutions used for monitoring diseases or patient movements.[88] Each of these scholars contributes to the tapestry of health app functions, recognising the varied roles these apps play in health promotion and disease management. However, none delve into establishing a formal classification scheme, leaving a gap for a methodological approach to organising health apps by function and purpose.

Yasini and Marchand have proposed a methodological approach to classifying health apps.[89] They categorised medical apps into six distinct categories: consulting medical information references; communication and information sharing; fulfilling a contextual need; educational tools; managing professional activities, and health related management. According to them this methodology enables users and healthcare professionals to navigate the complex health app landscape more effectively by aligning app functionalities with specific healthcare needs and contexts. Their classification acknowledges the diverse ways in which apps are integrated into healthcare and wellness. However, their classification falls short in addressing the tremendous diversification seen since in app capabilities and healthcare integration. Specifically, their framework overlooks entire emerging segments like health financing apps facilitating insurance claims and payments (e.g. Paymenow[90]), public health management apps enabling outbreak surveillance (e.g. HealthConnect[91]), pharmaceutical supply chain apps for medication inventory/delivery (e.g. PharmaGo[92]), and patient health records apps like HealthID[93] that exchange digitised treatment information with provider systems.

Their categories also do not incorporate the rise of mental health apps providing counselling, nor the growth in apps using personal data for customised diagnostics and predictive risk assessments. Furthermore, their segments are not differentiated by end-user groups, failing to distinguish apps specifically targeting patients, caregivers, providers and general wellness consumers - each having distinct needs. In essence, while valuable contextually, static classification systems have inherent limitations dealing with healthcare's dynamic technological transformation. As apps continue integrating diverse digital capabilities reshaping care access, updated categorisation methodologies are vital for stakeholders to comprehend the evolving landscape when selecting or prescribing tools matching specific requirements.

The global mHealth apps market is on a steep upward trajectory, with an expected growth to USD 105.9 billion by 2030. The sheer volume of health apps, with approximately 350,000 in major app stores and around 90,000 new ones added in 2020, presents an overwhelming challenge for South African users trying to select the right app. This explosion of digital health tools underscores the critical need for a systematic approach to classify and evaluate these apps in the local context. In developing a method to classify health apps, especially within the South African context, it is insightful to draw parallels with

[86] Erikson, S., 'COVID-19 Mobile Phone Apps Fail the Most Vulnerable', *Global Policy Journal* (2020).

[87] Arueyingho, O and Sanyaolu, K., 'Digital Health Promotion for Fitness Enthusiasts in Africa', IEEE International Conference on Digital Health, 2022.

[88] Miller, J.P., Sander, A and Srinivasav, S., 'Control, Extract, Legitimate: Covid-19 and Digital Techno-opportunism across Africa', *Development and Change,* 53:6 (2022), 1283-1307.

[89] Yasini M and Marchand G., 'Towards a use case-based classification of mobile health applications', *Studies in Health Technology and Informatics* (2015).

[90] https://bfaglobal.com/catalyst-fund/insights/meet-paymenow-a-financial-wellness-app-helping-south-africans-escape-debt-cycles-via-access-to-liquidity/

[91] https://www.exemplars.health/emerging-topics/epidemic-preparedness-and-response/digital-health-tools/healthconnect-in-south-africa

[92] https://disruptafrica.com/2021/08/06/sa-startup-pharmago-app-facilitates-fee-free-essential-medication-delivery/

[93] Reid, SJ et al., 'Do electronic patient information systems improve efficiency and quality of care? An evaluation of utilisation of the Discovery HealthID application' (2020) South African Medical Journal, Vol 110, N.3

the methodology developed by Kay[94] for categorising educational apps, albeit with necessary adaptations.

Kay's approach involves a detailed categorisation system, where educational apps are segmented into eight distinct categories: instructive, practice-based, metacognitive, constructive, productive, communicative, collaborative, and game-based. This classification is grounded in the functionality and educational objectives of the apps, allowing for a nuanced understanding of their utility in various learning contexts. Importantly, Kay's methodology extends beyond mere categorisation; it involves guidelines for selecting and evaluating apps based on critical factors such as the role of the educator, the intended learning outcomes, and the quality of content. This approach to app classification and evaluation, while tailored to the educational sector, provides a template for similarly dissecting the health app market. It underscores the importance of considering the specific roles and objectives of apps in their respective domains.

Applying a similar approach to the health app ecosystem in South Africa, it becomes evident that a nuanced classification system is required to cater to the diverse functionalities of health apps. In the South African context, health apps can be seeing as serving various purposes ranging from telemedicine, as seen in Hello Doctor, to health information platforms like HealthDart,[95] maternal health support through MomConnect, and health financing with apps like Paymenow. Each of these apps fulfils distinct health-related needs, mirroring the need for varied categories in Kay's educational app framework. The classification of health apps in South Africa, therefore, needs to be anchored in their functionalities and the specific health outcomes they aim to achieve. This approach would not only streamline the categorisation process but also aid users in selecting apps that align best with their health requirements and objectives, making the digital health landscape more navigable and effective.

Thus, applying a content analysis approach to the policies, laws, and regulations related to digital health in South Africa reveals essential keywords and concepts such as telemedicine, health information, disease monitoring, maternal and child health, mental health, insurance and health financing. This approach, combined with an understanding of the lived realities of South Africans, shapes a taxonomy for classifying health apps based on their functionalities and the health services they offer. The lived reality, including widespread internet penetration and the cultural context, plays a crucial role in categorising these apps. For instance, South Africa's high internet usage, with 43.48 million internet users as of early 2023 and an internet penetration rate of 72.3 percent, reflects a digitally engaged population.[96] The presence of 25.80 million social media users, amounting to 42.9 percent of the population, and a striking number of 112.7 million cellular mobile connections, exceeding the total population, underscores the deep integration of digital technology in daily life.[97]

This digital engagement has led to a significant number of people downloading a variety of apps, particularly health and fitness apps. The popularity of these apps is not just a reflection of their utility but also of the growing health and fitness consciousness among South Africans. Arueyingho and Sanyaolu have noted the increasing prevalence of fitness apps, catering to the growing number of fitness enthusiasts in Africa.[98] This trend indicates the need for a specific category dedicated to health and

[94] Kay, R., 'Creating a Framework for Selecting and Evaluating Educational Apps', *Proceedings of INTED2018 Conference* 5-7th March 2018.

[95] https://www.healthdart.co.za/

[96] DATAREPORTAL, DIGITAL 2023: South Africa, https://datareportal.com/reports/digital-2023-south-africa?rq=south%20africa

[97] DATAREPORTAL, DIGITAL 2023: South Africa, https://datareportal.com/reports/digital-2023-south-africa?rq=south%20africa

[98] Arueyingho, O and Sanyaolu, K., 'Digital Health Promotion for Fitness Enthusiasts in Africa', IEEE International Conference on Digital Health, 2022.

fitness apps within the broader taxonomy. Therefore, while developing the taxonomy, it is essential to consider not only the legal and policy framework but also the cultural and social contexts that influence app usage. This comprehensive approach ensures that the classification of health apps is aligned with both the regulatory environment and the actual usage patterns and preferences of the South African population. Therefore, in incorporating these insights into the categorisation process the following taxonomy can be developed that classifies these apps into specific categories based on their functionalities and the health services they provide:

a. Telemedicine Apps: Enable virtual physician consultations and remote healthcare services. Examples include Hello Doctor,[99] Kena Health,[100] Quro Medical[101].

b. Health Information Apps: Share knowledge resources on symptoms, diseases, and self-care practices. Examples include MomConnect,[102] HealthDart.[103]

c. Patient Health Records Apps: Digitise, exchange, and monitor longitudinal patient treatment data. Examples include Vula Mobile,[104] Vantage App,[105] and HealthID.[106]

d. Health & Wellness Apps: Focus on tracking fitness, biometrics, and providing lifestyle change nudges. Examples include Fitbit, Twilight, Strave, Sleep, My Fitness Pal.[107]

e. Personal Health Monitoring Apps: Capture individual health data for self-surveillance, such as period trackers, diabetes management apps.

f. Diagnostic/Clinical Reference Apps: Use risk stratification algorithms or care guidelines to aid health assessments. Example SAMF App.[108]

g. Pharmaceutical Supply Chain Apps: Focus on medication delivery prescribed through virtual/remote consultation and inventory tracking. Example PharmaGo.[109]

h. Health Financing Apps: Facilitate insurance policy purchases, premium payments, and claims processing. Example Paymenow.[110]

i. Public Health Management Apps: Streamline surveillance, outbreak predictions, and data visualization for responsive public health interventions. Example COVID Alert SA App.[111]

This proposed taxonomy serves as a valuable starting point for understanding and evaluating South Africa's health app ecosystem. By categorising apps into distinct groups, it provides a clear framework

[99] https://www.hellodoctor.co.za/
[100] https://www.kena.health/
[101] https://www.quromedical.co.za/
[102] https://www.health.gov.za/momconnect/
[103] https://www.healthdart.co.za/
[104] https://www.vulamobile.com/
[105] https://broadreachcorporation.com/together-we-will-conquer-mpumalanga-launches-mobile-app-to-stop-covid-19-spread/
[106] Reid, SJ et al., 'Do electronic patient information systems improve efficiency and quality of care? An evaluation of utilisation of the Discovery HealthID application' (2020) South African Medical Journal, Vol 110, N.3
[107] https://longevitylive.com/regions/africa/top-10-most-popular-health-apps-in-south-africa/
[108] https://play.google.com/store/apps/details?id=com.aviro.samf&hl=en&gl=US
[109] https://disruptafrica.com/2021/08/06/sa-startup-pharmago-app-facilitates-fee-free-essential-medication-delivery/
[110] https://bfaglobal.com/catalyst-fund/insights/meet-paymenow-a-financial-wellness-app-helping-south-africans-escape-debt-cycles-via-access-to-liquidity/
[111] https://www.discovery.co.za/corporate/download-covid-alert-sa-app-today

for users, healthcare providers, researchers, and policymakers to navigate the diverse landscape of digital health solutions. The taxonomy facilitates the selection of appropriate apps based on specific needs and objectives while laying the groundwork for comparative analysis within and across categories. The proposed taxonomy for classifying health apps in South Africa encompasses both locally developed apps by South African companies as well as apps developed by foreign companies that have been adopted for use locally (like Kena Health developed by Cardo Health which is a Swedish based healthcare startup[112]). This interplay between homegrown innovations and the adoption of foreign solutions has important legal implications.

For locally developed apps, the regulatory framework and data protection laws in South Africa would be directly applicable. Developers would need to ensure compliance with regulations such as the Protection of Personal Information Act (POPIA) and any specific guidelines or policies related to digital health and the handling of sensitive medical data. However, for foreign apps being used in South Africa, there may be jurisdictional complexities and potential conflicts between South African laws and the laws of the app's country of origin. This could lead to situations where a foreign app's data practices or terms of service may not fully align with South African regulations, potentially exposing users to data privacy risks or limiting their legal recourse in case of violations. Additionally, the cross-border transfer and storage of personal health data by foreign apps may raise concerns about data sovereignty and the applicability of South African laws.

Furthermore, locally developed apps may have a better understanding of the specific cultural, linguistic, and contextual nuances of the South African healthcare landscape, potentially making them more tailored and appropriate for local users. In contrast, foreign apps developed by teams without direct exposure to the South African context may struggle to capture these nuances accurately. Their design and functionality may inadvertently reflect biases or assumptions rooted in their cultural backgrounds, potentially leading to misalignments or usability issues for South African users. For instance, an app developed in a Western context may prioritise individualistic approaches to healthcare, while many South African communities prioritise communal or family-centric approaches. Such disconnects can create barriers to adoption and undermine the app's effectiveness in addressing local healthcare needs.

For example, this disparity is exemplified by the case of Cardo Health, a Swedish startup that has developed Kena Health. Their team composition, consisting of 11 white males, 1 Asian male, and 3 females, highlights a potential lack of diversity and representation that could lead to inherent biases in the app's design and functionality.[113] A homogeneous team, primarily comprising individuals from a specific cultural background, may inadvertently overlook or misinterpret the nuances and realities of diverse populations, including those in South Africa. In reviewing Cardo Health's website, I observed that the lack of gender, racial, and ethnic diversity within team.

While international collaborations and knowledge sharing can help bridge the gap between foreign and locally developed apps, there are risks associated with adopting blueprints or models from foreign companies. One significant concern is the potential for enabling surveillance, user tracking, and unauthorised data sharing practices within South Africa's health app ecosystem. This issue has been flagged by Mckay et al,[114] Brand et al,[115] and Barit.[116] Foreign companies may have different data privacy standards, regulatory environments, or business models that prioritise data collection and monetisation. If their app blueprints are adopted by local developers without proper scrutiny or adaptation, it could lead to the integration of questionable data practices into South African health apps.

[112] https://nordic9.com/news/cardo-health-raised-sek-150-million/

[113] https://www.cardohealth.com/our-team

[114] Mckay AGN, Brand D, Botes M et al, 'The regulation of health data sharing in Africa: a comparative study' (2024) *Journal of Law and the Biosciences*, Vol 11, Issue 1.

[115] Brand D, McKay AGN and Cengiz N, 'What constitutes adequate legal protection for the collection, use and sharing of mobility and location data in health care in South Africa', (2022) *S Afr J Sci* 119(5/6).

[116] Barit A, 'The apps are coming! But will they be legal in South Africa?', *S Afr Med J* 2019; 109(3):150-151.

For instance, Masood et al have argued that some foreign app models may incorporate extensive user tracking mechanisms or data-sharing agreements with third-party entities for purposes such as targeted advertising or analytics.[117] While these practices may be deemed acceptable or regulated differently in the app's country of origin, they could violate data privacy laws or public expectations in South Africa, particularly when dealing with sensitive health information. Moreover, foreign companies' data storage and processing infrastructures may be located outside of South Africa, raising concerns about data sovereignty and the applicability of local data protection laws. Users' personal health data could potentially be subjected to foreign jurisdictions with weaker privacy regulations, exposing them to greater risks of unauthorised access or misuse. Additionally, the terms of service or privacy policies crafted by foreign companies may not align with the legal and ethical standards expected in South Africa's healthcare domain. These policies could grant broad permissions for data collection, sharing, or use, which may conflict with the principles of informed consent and individual autonomy over personal health information.

2.2.4. Techno-Legal Factors Impacting the Apps Ecosystem

This section continues the discussion of the health apps ecosystem by delving deeper into analysing their financing and funding flows, target user segments, and the adoption patterns of these apps. It also examines aspects of the apps' intellectual property and control as part of the digital economy, especially in relation to the interdependencies of health apps with digital payment platforms and mobile banking through which online consultation, e-prescriptions, payments, health records are all connected. The dynamics of financing, funding flows, target segments, and intellectual property arrangements underpinning health apps align closely with key tenets of assemblage theory.[118] Assemblages consist of heterogeneous elements and complex interrelationships that shape collective behaviours. Similarly, apps draw lifeblood from diverse financial sources, respond to varied user needs, and balance tensions between open collaborative innovation and proprietary knowledge control.[119]

Therefore, viewing apps as socio-technical assemblages illuminates the multidirectional interdependencies between external investment inflows seeking returns, patient expectations determining feature priorities, developer capabilities enabling functionality, and policy efforts to balance public good with profit drivers. Farlow et al observe that apps morph as these variables flux, their form and purpose shaped by realignments in funding availability, user segments, competitive forces, regulations around data protection, and priorities of participating human and non-human actors.[120]

For instance, Swartz et al reveal that many South African health apps rely considerably on foreign capital inflows, accumulating financial assemblages spanning investor locales from the Global North.[121] Birhane explains that such dependence on external shareholders complicates local control,[122] potentially concentrating value outside health systems that most apps ostensibly aim to strengthen. This imbalance

[117] Masood R, Berkovsky S and Kaafar MA, 'Tracking and Personalisation' (2021) In: Knijnenburg, B.P., Page, X., Wisniewski, P., Lipford, H.R., Proferes, N., Romano, J. (eds) *Modern Socio-Technical Perspectives on Privacy.* Springer, Cham.

[118] Ian Buchanan, *Assemblage Theory and Method* (Bloomsbury Publishing, 2020).

[119] Foster C., 'Intellectual property rights and control in the digital economy: Examining the expansion of M-Pesa', *The Information Society*, vol 40, no.1 (2024), 1-17.

[120] Farlow A, Hoffman A, Tadesse GA et al., 'Rethinking global digital health and AI for health innovation challenges', *PLOS Glob Public Health* 3:4(2023); Hellstrom J., 'The Innovative Use of Mobile Applications in East Africa' Sida (2010).

[121] Swartz A, LeFevre A, Perera S et al, 'Multiple pathways to scaling up and sustainability: an exploration of digital health solutions in South Africa' (2021) *Global Health* 17, 77.

[122] Birhane A., 'Algorithmic Colonisation of Africa' In Stephen Cave and Kanta Dihal (eds), *Imagining AI: How the World Sees Intelligent Machines* (Oxford Academic, 2023).

highlights assemblage precarity arising from incongruent incentive alignment between commercial backers seeking maximised returns and public stakeholders prioritising equitable access or welfare externalities. Furthermore, while open-source collaborative models allow decentralised participation in software development, app ownership centralisation can undermine such democratisation promises in practice.[123] Consequently, investor demands, and proprietary constraints forestall user liberties customising code or data to suit local contextual needs. Such resulting exclusion, argue Freuler,[124] and Loo[125] economically disempowers non-elite software talent pools, even while apps penetrate widely due to the ubiquity of mobile devices. According to them the creative localised innovation then remains thwarted by financial, skill and legal gatekeeping. There is an existing gap in the literature around these manifestations when examining health apps in South Africa.

The FTI Consulting report on the 'Overview of the health technology sector in South Africa'[126] highlights the country's reliance on imported medical devices and technologies, with an estimated 90% of the medical technology currently used in South Africa being imported. This reliance on foreign technologies for health apps raises concerns about data sovereignty, as personal health data collected through these apps may be stored, processed, or managed outside South Africa's borders. Donnelly[127] underscores this concern, stating that the Medicines and Related Substances Act 101 of 1965 defines 'medical device' broadly, potentially encompassing software intended for diagnosis, treatment, or monitoring of diseases. This suggests that foreign health apps could fall under this definition, potentially subjecting them to South Africa's data protection regulations. However, the cross-border transfer of data through these apps may challenge South Africa's ability to exercise data sovereignty and enforce its data localisation principles.

The FTI Consulting report also notes that local production of medical devices in South Africa is primarily limited to low-tech consumables, while more sophisticated technologies are imported. This implies that health apps developed by foreign companies are likely to involve proprietary algorithms, software, and technologies protected by intellectual property rights. Relatedly, Donnelly's also highlights the IP concerns surrounding health apps, stating that foreign companies may seek to protect their innovations through patents, copyrights, or trade secrets. This raises questions about the extent to which South Africa can ensure access to essential healthcare technologies and strike a balance between respecting IP rights and promoting public health interests.

The potential commercialisation of personal health data collected through foreign health apps is a significant concern in the South African context. Donnelly warns that personal health data could be commercialised for profit-making purposes by foreign entities, potentially compromising the privacy and autonomy of South African citizens. Furthermore, Klingberg et al[128] in their study on designing digital maternal and child health solutions in Soweto reveals concerns among participants about the cost and accessibility of technology-based solutions, as well as the risks associated with crime and theft of devices. These concerns highlight the potential barriers to equitable access to health apps, especially if foreign companies prioritise commercialisation over affordability and local context. Additionally,

[123] Ibid.

[124] Freuler, JO., 'Unveiling Gatekeeping Practices in Mobile Environments: A Comparative Analysis of Operating Systems and App Gardens', *International Journal of Communication*, Vol 17 (2023).

[125] Loo RV, 'The New Gatekeepers: Private Firms as Public Enforcers', *Virginia Law Review*, Vol 106, No. 2 (2020), 467-522.

[126] FTI Consulting, 'Overview of the health technology sector in South Africa: opportunities for collaboration' (2019) Commissioned by the Netherlands Enterprise Agency

[127] Donnelly DL, 'First Do No Harm: Legal Principles Regulating the Future of Artificial Intelligence in Health Care in South Africa" *PER / PELJ* 2022(25))

[128] Klingberg S, Motlhatlhedi M, Mabena G, Mooki T, Verdezoto N, Densmore M, et al. "Must you make an app?" A qualitative exploration of socio-technical challenges and opportunities for designing digital maternal and child health solutions in Soweto, South Africa' (2022) *PLOS Glob Public Health* 2(12)

Rambe and Maime[129] emphasise the challenges of enforcing South African laws and regulations on multinational corporations operating across multiple jurisdictions. This raises concerns about the effective enforcement of data protection laws, such as the Protection of Personal Information (POPIA) Act, in the context of foreign health apps.

The reliance on foreign technologies and software for health apps in South Africa raises significant concerns about data sovereignty and data localisation. As highlighted by Brand et al,[130] this reliance effectively cedes a degree of control over the storage, processing, and management of sensitive personal health data to entities operating outside South Africa's jurisdiction. Brand et al argue that the lack of comprehensive legal frameworks and guidelines specifically tailored to the unique challenges posed by health apps and mobile data collection. While South Africa's Protection of Personal Information Act (POPIA) provides a general framework for data protection, it may not adequately address the specific nuances and risks associated with health data collected through mobile apps. The absence of clear guidelines on obtaining informed consent, ensuring data security, and regulating cross-border data transfers can create uncertainties and potential loopholes that may compromise user privacy.

The use of health app data in conjunction with other data sources, such as insurance records or government databases, raises further concerns about data linkage, profiling, and potential discrimination.[131] Another key issue is the potential for health apps to reproduce or exacerbate existing power imbalances between app developers, healthcare providers, and individual users. The terms and privacy policies of health apps often advantage app owners and data processors, leaving users with limited negotiating power or recourse in case of data breaches or misuse.[132] The complexity and length of these policies can make it difficult for users to fully understand their rights and the implications of sharing their health data.[133]

The open-source software deployment in the public sector, as discussed by Mutula and Kalaote[134], offers a potential avenue for addressing some of these concerns. By promoting transparency, interoperability, and local capacity building, open-source solutions can help to create more accountable and user-centric health app ecosystem. The case of Pelebox,[135] a locally developed digital platform in South Africa is a good example, which highlights several important lessons specific to the South African context in terms of health app development, deployment, and potential impact on the healthcare system from the perspective of open source software.

Firstly, Pelebox demonstrates the potential for locally developed health apps to address unique challenges faced by the South African healthcare system, such as long waiting times and overcrowding at public clinics. By leveraging technology to streamline medication collection processes, Pelebox showcases how innovative solutions can be tailored to meet the specific needs of the South African population. This underscores the importance of fostering a vibrant local app development ecosystem that can respond to the country's healthcare challenges with context-specific solutions. Secondly, the partnership between Pelebox, the Technology Innovation Agency, Tshimologong (Wits University's digital innovation hub), and the Irish embassy highlights the value of collaboration between local developers, academic institutions, government entities, and international partners. This collaborative approach facilitates knowledge sharing, access to resources, and the opportunity for local start-ups to

[129] Rambe P and Maime R., 'The Impact of 4IR Technologies on Venture Creation and Technology Commercialisation: Insights and Exemplars from an Emerging Economy Context' In R. E. Hinson et al. (eds.), Small Business and Entrepreneurial Development in Africa (Springer, 2022)

[130] Brand, D., Nienaber McKay, A. G., & Cengiz, N, 'What constitutes adequate legal protection for the collection, use and sharing of mobility and location data in health care in South Africa?' (2023) *South African Journal of Science*, 119(5/6)

[131] Ibid.

[132] Ibid.

[133] Supra, n 124.

[134] Mutula, S., & Kalaote, T, 'Open source software deployment in the public sector: a review of Botswana and South Africa', (2010) *Library Hi Tech*, 28(1), 63-80.

[135] https://mg.co.za/health/2024-02-25-south-african-tech-entrepreneur-solves-health-problem/

scale their solutions and attract funding. Such partnerships can play a crucial role in nurturing and supporting the growth of the local health app industry in South Africa.

However, the reliance on data by platforms like Pelebox also raises important questions about data privacy, security, and governance. As patient data is collected, stored, and processed by these apps, it is crucial to ensure that appropriate safeguards are in place to protect sensitive health information. This requires a robust legal and regulatory framework that addresses the specific challenges posed by health apps and ensures compliance with data protection laws such as the Protection of Personal Information Act (POPIA). Moreover, the success of locally developed apps like Pelebox underscores the need for a supportive policy environment that encourages innovation and entrepreneurship in the digital health space. This may include initiatives such as funding opportunities, tax incentives, and streamlined regulatory processes that enable local start-ups to develop and deploy their solutions more effectively. The case of Pelebox also highlights the potential for health apps to contribute to the broader goals of universal health coverage and health equity in South Africa. By improving access to essential medicines and reducing waiting times, such apps can help to address some of the barriers to healthcare faced by vulnerable and underserved populations. However, it is important to ensure that the benefits of these technologies are distributed equitably and that they do not exacerbate existing health disparities.

2.2.5. Lessons Learnt

The analysis of the health apps landscape in South Africa, encompassing the categorisation of apps, techno-legal factors, and the risks associated with dependence on foreign systems, has revealed several crucial gaps in knowledge and practice. These gaps underscore the complex challenges faced by South Africa in navigating the rapidly evolving digital health ecosystem while ensuring the protection of citizens' rights and the integrity of the healthcare system.

One significant gap identified is the absence of a comprehensive and context-specific regulatory framework tailored to address the unique challenges posed by health apps and mobile data collection. While South Africa's Protection of Personal Information Act (POPIA) provides a general foundation for data protection, it may not adequately capture the nuances and risks specific to health data collected through mobile apps. The lack of clear guidelines on informed consent, data security, and cross-border data transfers creates uncertainties and potential vulnerabilities that could compromise user privacy and data sovereignty.

Moreover, the analysis highlights the limited understanding of the effectiveness and impact of health apps on health outcomes and healthcare delivery processes in the South African context. The paucity of evidence-based studies assessing the efficacy of these digital interventions hinders the development of informed policies and regulations. Without a robust evidence base, policymakers and healthcare providers may struggle to make informed decisions about the adoption, recommendation, or integration of health apps into the healthcare system.

The proposed taxonomy for classifying health apps in South Africa reveals the complex interplay between locally developed apps and those created by foreign entities. This dichotomy raises concerns about jurisdictional conflicts, data sovereignty, and the potential misalignment of foreign apps with South African cultural, linguistic, and contextual nuances. The lack of diversity and representation within the development teams of foreign apps may inadvertently perpetuate biases and assumptions that fail to capture the unique needs and preferences of South African users.

The reliance on foreign technologies and software for health apps in South Africa also exposes significant risks related to data sovereignty and localisation. The storage, processing, and management of sensitive personal health data by entities operating outside South Africa's jurisdiction effectively cedes a degree of control and raises questions about the applicability and enforcement of domestic data protection laws. The potential for cross-border data transfers and the commercialisation of personal health data by foreign entities further exacerbates concerns about privacy, autonomy, and the balance between intellectual property rights and public health interests.

The analysis also underscores the potential for health apps to reproduce or exacerbate existing power imbalances between app developers, healthcare providers, and individual users. The complexity and opacity of terms and privacy policies often advantage app owners and data processors, leaving users with limited understanding of their rights and the implications of sharing their health data. This asymmetry of power and knowledge raises ethical concerns about informed consent, data ownership, and the potential for exploitation or misuse of personal health information.

Furthermore, the examination of the health app ecosystem in South Africa reveals the challenges associated with equitable access and affordability. The reliance on imported technologies and the potential for commercialisation of health data by foreign entities may create barriers to access, particularly for marginalised or economically disadvantaged populations. The cost of devices, data, and subscription fees associated with health apps may exacerbate existing health disparities and widen the digital divide.

2.3. The Case of MomConnect, Kena Health and Ada

2.3.1. Method of Analysis

To examine the legal frameworks governing the MomConnect initiative, the Kena Health app, and the Ada app, this analysis employs a combination of literal and purposive interpretative approaches.nBy employing this combined literal and purposive approach, the analysis can generate a multi-layered understanding of the risks, challenges, and tensions inherent in the legal frameworks governing these digital health platforms. This holistic assessment can uncover transparency omissions, consent violations, and power imbalances that may undermine user rights, data sovereignty, and equitable platform governance, despite the formal articulation of user protections and empowerment.

2.3.2. Legal Analysis of MomConnect and Kena Health Contractual Terms and Privacy Policy

2.3.2.1. MomConnect

The MomConnect initiative leverages existing communication channels like SMS and WhatsApp to deliver its services.[136] This approach of utilising pre-existing technological infrastructures raises several legal considerations and potential issues that warrant critical analysis. One of the primary concerns stems from the lack of a dedicated website or platform for MomConnect, where its terms of service and privacy policies could be explicitly outlined. Instead, the initiative relies on the terms and conditions of the underlying communication channels it employs, namely the network providers for SMS services and WhatsApp's terms of service for its messaging component.[137] This reliance on third-party terms and conditions creates a complex legal landscape, as MomConnect's operations become subject to the policies and regulations set forth by these external entities. Consequently, the initiative may face challenges in ensuring complete transparency and clarity regarding data handling practices, user rights, and liability limitations specific to its context.

The use of SMS services implies that MomConnect's users are bound by the terms and conditions of their respective network providers. These terms can vary significantly across different providers, leading to potential inconsistencies in the legal framework governing the initiative's operations and user agreements. Such inconsistencies could result in disparities in data privacy protections, consent

[136] Skinner D., Delobelle, P., Pappin, M., et al., 'User assessments and the use of information from MomConnect, a mobile phone text-based information service, by pregnant women and new mothers in South Africa', (2018) *BMJ Global Health* 3(S2): 1-6.
[137] https://measured.design/momconnect/

mechanisms, and liability clauses, depending on the user's network provider. Similarly, the integration of WhatsApp into MomConnect's services introduces another layer of complexity, as users are subject to WhatsApp's terms of service and data policies. While WhatsApp's terms may provide a more standardised legal framework, there is a risk of conflicts or gaps between WhatsApp's policies and the specific requirements or objectives of MomConnect's health-related services. Furthermore, the sharing and potential co-mingling of users' data across multiple infrastructures raise concerns about data ownership, control, and accountability. This analysis is grounded in the discussions and observations made by Kostkova et al[138] who highlight the complex and disparate landscape surrounding data ownership and usage in the healthcare domain, noting the emergence of two distinct approaches in the absence of transparent data ownership regulation.

On one hand, Kostkova et al discuss the government-regulated clinical and research medical data, including individual and population data gathered by non-governmental organisations. Here, they note that poor government communication, unclear agendas, and lack of transparency over the control and ownership of medical data have led to a loss of citizen trust. On the other hand, the authors point out that some citizens seem less concerned about their user-generated health data being directly collected by IT and social media companies, as well as MedTech manufacturers, through tracking/wearable devices and social media. This data is often collected with commonly no opt-out options, potentially subjecting individuals to personal intrusion through data analytics-driven marketing and unregulated sharing and use.

The juxtaposition of these two approaches raises important questions about the motivations and awareness of citizens who find themselves at the intersection of these data collection and usage practices. The authors suggest that the matter may be more complex than a simple lack of awareness, as citizens may feel that their explicit consent is required for data sharing in the former group (where the data are extracted from clinical records), while they may have agreed to sharing with the IT and MedTech industry in the second group (where the user-generated content could be considered donated by accepting terms and conditions). Ultimately, the authors underscore that beyond the issue of ownership and consent for sharing data, the more pressing concern may be the question of who is using the shared citizens' data and for what purposes, and how such decisions could be effectively controlled by citizens themselves. The sharing and potential co-mingling of users' data across multiple infrastructures, both government-regulated and privately owned, raise critical questions about data ownership, control, and accountability that require further examination and policy intervention.

Consequently, it becomes challenging to establish clear lines of responsibility and liability in cases of data breaches, unauthorised access, or misuse of personal information, as the data may traverse multiple systems and entities. Additionally, the lack of a dedicated platform for MomConnect limits the initiative's ability to tailor its legal agreements and policies to align with specific healthcare regulations, data protection laws, or ethical guidelines that may govern the handling of sensitive health information. Relying on third-party terms and conditions may not adequately address the unique legal and regulatory requirements associated with healthcare services and the management of personal health data.

The analysis of the MomConnect initiative's approach to leveraging existing communication channels like SMS and WhatsApp can be contextualised within the broader discussion on digital platforms as discussed by Msiska et al.[139] These authors highlight the pervasive nature of digital platforms, which have transformed various spheres of modern life, including the healthcare industry. Specifically, they discusses the concept of digital platforms as modular systems comprising a set of stable core components and a complementary set of variable peripheral components. In the case of MomConnect,

[138] Kostkova P et al, 'Who Owns the Data? Open Data for Healthcare' (2016) 4 *Frontiers in Public Health* 7.

[139] Msiska B, Nielsen P and Kaasboll J, 'Leveraging digital health platforms in developing countries: the role of boundary resources', In: Nielsen, P., Kimaro, H.C. (eds) *Information and Communication Technologies for Development. Strengthening Southern-Driven Cooperation as a Catalyst for ICT4D.* ICT4D 2019. IFIP Advances in Information and Communication Technology, vol 551. Springer, Cham.

the initiative relies on pre-existing technological infrastructures, such as SMS and WhatsApp, as the peripheral components that extend the core functionality of the platform. The authors also emphasise the role of boundary resources, which facilitate the relationship between platform owners and external actors leveraging the platform to create derivative innovations. In the case of MomConnect, the lack of a dedicated website or platform means that the initiative is subject to the terms and conditions of the underlying communication channels it employs, namely the network providers for SMS services and WhatsApp's terms of service.

This reliance on third-party terms and conditions raises several legal considerations and potential issues. The complex legal landscape created by this approach may challenge MomConnect's ability to ensure complete transparency and clarity regarding data handling practices, user rights, and liability limitations specific to its context. This aligns with the Msiska et al's observation that boundary resources, such as APIs and SDKs, play a significant role in the leveraging of digital health platforms in developing countries. Their discussion of generative collectives and the collective generative capacity of individuals within these collectives is also relevant to the MomConnect analysis. The initiative's approach of utilising pre-existing technological infrastructures may have implications for the generative capacity of the individuals and communities involved, as the boundary resources (or lack thereof) may influence their ability to innovate and create derivative applications on top of the platform.

2.3.2.2. Kena Health

The discussion surrounding the Kena Health app[140] presents additional complexities in the context of digital health platforms and their legal implications, particularly in developing country settings. Similar to the MomConnect initiative, Kena Health also relies on leveraging existing technological infrastructure, in this case, requiring users to register using a valid South African ID. However, the lack of publicly accessible terms of service and privacy policy documentation for both the Kena Health app and its parent company, Cardo Health,[141] raises significant concerns. The absence of readily available information on the legal and data handling practices of these digital health platforms poses a critical challenge. Users are effectively prevented from understanding the full extent of their rights, the data protection measures in place, and the potential liabilities associated with the use of these services. This opacity undermines the principles of transparency and informed consent, which are essential for building trust and ensuring the ethical deployment of digital health technologies, particularly in developing country contexts where access to digital services may be limited.

From an academic perspective, this issue aligns with the Msiska et al's discussion of boundary resources and their role in facilitating the leveraging of digital health platforms.[142] The lack of clear and accessible boundary resources, such as terms of service and privacy policies, creates a barrier to understanding the legal and regulatory frameworks governing the use of these platforms. This, in turn, can hinder the collective generative capacity of the individuals and communities involved, as they may be unable to fully engage with and build upon these digital health solutions in an informed and empowered manner. Furthermore, the foreign ownership and development of the Kena Health app by Cardo Health raises additional concerns regarding the potential power dynamics and asymmetries inherent in the international division of labour within the digital platform ecosystem. Msiska et al's observation that many contemporary digital platforms originate or are developed in developed countries and subsequently appropriated for use in developing countries is particularly relevant here. The opacity surrounding the legal and data handling practices of Kena Health and Cardo Health may exacerbate this imbalance, potentially compromising the agency and self-determination of local communities in the development and deployment of digital health solutions.

[140] https://www.kena.health/
[141] https://www.cardohealth.com/
[142] Supra, n 137.

The analysis presented by Binns et al[143] on the prevalence of third-party tracking in the mobile ecosystem provides a valuable framework for understanding the Kena Health app in the absence of its terms and privacy policy. Their empirical study of nearly 1 million apps from the Google Play Store sheds light on the complex legal and ethical considerations surrounding the use of third-party tracking technologies, particularly in the context of digital health platforms. They argue that the lack of publicly accessible terms of service and privacy policy documentation creates significant barriers to understanding the legal and data handling practices of apps. As the authors note, the absence of readily available information on user rights, data protection measures, and potential liabilities undermines the principles of transparency and informed consent - essential components for building trust and ensuring the ethical deployment of digital health technologies.

Furthermore, Binns et al's analysis of the differences in third-party tracker prevalence across various app genres provides important context for understanding the potential challenges posed by the Kena Health app. As a health-focused app, one might expect a higher degree of privacy and data protection measures. However, the lack of transparency around the app's terms and conditions suggests that users may not be fully aware of the extent to which their personal data is being collected and shared with third parties - a concern that is amplified by the authors' findings that news and family-oriented apps exhibit the highest number of trackers. Addressing these issues is crucial, as the authors argue, for ensuring the responsible and equitable development and deployment of digital health solutions, particularly in developing country contexts. The opacity surrounding the Kena Health app and Cardo Health's practices prevents a comprehensive understanding of the legal issues and user rights associated with these platforms, ultimately undermining the principles of transparency, informed consent, and the collective generative capacity of the communities they aim to serve.

2.3.2.3. Ada

The Ada app is developed by the German-based Ada Health GmbH. A doctrinal review of Ada's terms[144] of service through literal and purposive analysis reveals concerns regarding outsized centralization of proprietary controls, expansive third-party data sharing devoid of accountability, and overreaching limitations to legal liability. At the outset, the terms codify sweeping assertions of intellectual property monopoly over the software, algorithms, and content constituting the Ada app exclusively to the parent Ada Health GmbH entity and its undisclosed affiliates. This proprietary dominance severely hampers any user participation freedoms to request even trivial modifications such as user interface localisation that could enhance cultural relevance. The restrictive stipulations effectively functioning as a technology gatekeeper reveal tensions within aspirations positioning apps as progressively advancing accessibility.

Furthermore, the terms grant Ada expansive rights to harness anonymised user data in perpetuity without limits or transparency over subsequent analysis practices. This blanket data usage license suggests accumulation of population-scale information stocks for profiling, clustering, and secondary research purposes that contravene principles of purpose limitation. The data sovereignty risks get compounded by interoperability permissions allowing silent transfer of personal social media content like birth dates once app users sign-in via Google. Further, clause 12.3 of Ada's terms contain a presumption of consent to updated terms if the user does not explicitly object within 30 days of receipt of amendments. This obfuscates continuous consent withdrawal rights.

Under clause 3.2, Ada retains a perpetual license to utilise anonymised user data without limits. This signifies data accumulation for analysis, profiling, and secondary commercialisation absent transparency guarantees. There are also sweeping exclusions of legal liability for platform errors under

[143] Binns R, Lyngs U, Kleek M., et al, 'Third Party Tracking in the Mobile Ecosystem', (2018) In WebSci '18: 10th ACM Conference on Web Science, May 27–30, 2018, Amsterdam, Netherlands. ACM, New York, NY, USA,

[144] https://ada.com/terms-and-conditions/

clause 9.4, which indicate severe erosion of user accountability from dependencies on privately controlled infrastructure for healthcare access. These terms effectively erode consumer recourse or compensatory avenues despite deepening dependencies on privately controlled infrastructure for healthcare access.

Further analysis of the Ada app's terms and conditions reveal several potential legal loopholes and concerns, particularly in the context of its availability in South Africa as a result of a collaboration between Praekelt (now known as Reach Digital Health) and the Rockefeller Foundation. One of the primary issues is the lack of transparency and user control surrounding the app's data sharing practices and third-party involvement. The terms do not provide clear information about how users' personal data may be used and shared (clause 3.1, 3.2), making it difficult for individuals to understand the implications of engaging with the app. The broad language around the right to use 'anonymised' data in perpetuity, coupled with the absence of explicit user control over this process (clause 3.2), raises significant concerns about the protection of users' privacy and autonomy.

Another area of concern is the unclear jurisdiction and applicable law governing the agreement. The terms state that the contract is subject to German law (clause 14.1), which may not align with the local laws and regulations in South Africa, where the app is being used. This discrepancy in jurisdiction and applicable law could create challenges for South African users in terms of enforcing their rights and seeking redress for any potential issues that may arise. The terms also raise questions about the limitations on user responsibilities and liabilities. While the terms extensively outline the user's responsibilities and prohibitions (clause 7.2), the language around Ada's liabilities and the consequences for users is relatively vague and limited (clause 9.4). This imbalance in the allocation of responsibilities and liabilities could disproportionately burden the users, especially in cases of adverse health outcomes or misuse of the app's services.

Additionally, the terms provide limited details on the conditions and procedures for terminating the user's agreement and deleting their personal data (clause 8.5). This lack of clarity could leave users uncertain about their rights and the protection of their data upon termination of the agreement. Another significant concern is the absence of any specific dispute resolution mechanisms, such as an internal grievance process or a referral to an independent ombudsman (clause 14.3). This could make it challenging for users to address any issues or complaints they may have regarding the app's services or data practices.

When it comes to Ada's privacy policy[145] it reveals several potential legal loopholes and areas of concern, despite its attempts to provide a comprehensive overview of the company's data processing practices. One significant issue is the broad and permissive language around the company's right to use anonymised user data in perpetuity. The policy grants Ada expansive rights to accumulate and analyse this anonymised information, without providing clear limitations or transparency on how this data may be utilised, including for potential secondary research or commercialisation purposes (clause 3.2). This raises questions about the true anonymity of the data and the extent of user control over their personal information.

Another area of concern is the reliance on third-party service providers, both within the EU and in the United States, to process user data. While Ada claims to have appropriate safeguards in place, such as standard contractual clauses, the policy lacks specific details on the nature and extent of these measures (clause 6.1). The Schrems II decision by the Court of Justice of the European Union has called into question the adequacy of such mechanisms for data transfers to the US, adding uncertainty to the legality of these arrangements.[146] The policy also contains provisions that allow Ada to disclose user data in the

[145] https://ada.com/privacy-policy/

[146] Kowalski J, 'Schrems II: Privacy Shield faces same demise as Safe Harbor. Uncertain future for Standard Contractual Clauses for US transfers', (2020); https://www.dacbeachcroft.com/what-we-think/Schrems-II-Privacy-Shield-faces-same-demise-as-Safe-Harbor-Uncertain-future-for-Standard-Contractual#:~:text=The%20court%20has%20decided%20that,Economic%20Area%20to%20the%20US.

event of a business acquisition or sale of assets (clauses 6.3 and 6.4).. While this may be a legitimate business interest, the lack of explicit user consent and the potential for sensitive health data to be transferred to unknown third parties is troubling from a data protection standpoint.

Furthermore, the policy's treatment of user rights, such as the right to object or the right to data portability, is somewhat limited in its scope and clarity. For example, the policy does not provide detailed instructions on how users can exercise these rights, nor does it address potential challenges or limitations in fulfilling such request (clause 8). s. Finally, the policy's approach to obtaining user consent, particularly for the processing of sensitive health data, raises concerns. While the policy states that consent is required for certain processing activities, the language around the presumption of consent to updated terms if a user does not object within 30 days is concerning, as it may undermine the user's continuous right to withdraw consent (clause 12.3).

Overall, while Ada's privacy policy appears to make an effort to comply with relevant data protection regulations, such as the General Data Protection Regulation (GDPR) and local laws, the presence of these legal loopholes and ambiguities may expose users to potential risks and limit their ability to exercise meaningful control over their personal information.

2.3.3. Lessons Learned

The analysis of the contractual terms and privacy policies governing MomConnect, Kena Health, and the Ada app has revealed several key lessons and identified important knowledge gaps that warrant further research in the domain of digital health platforms and their legal and regulatory implications, particularly in developing country contexts.

One of the overarching lessons learned is the critical importance of transparency, user control, and alignment with data protection principles in the deployment of digital health technologies. The reliance of MomConnect and Kena Health on pre-existing communication channels and infrastructure, without dedicated platforms and clearly delineated terms of service and privacy policies, has created complex legal landscapes that undermine the principles of transparency and informed consent. This opacity prevents users from fully understanding the scope of data handling practices, their rights, and the potential liabilities associated with the use of these services. The analysis of the Ada app has further corroborated these concerns, highlighting the broad and permissive language around data usage, the ambiguity in user rights, and the overreaching limitations on legal liability.

These findings underscore the need for digital health platforms to prioritise the development of dedicated, user-centric platforms and legal agreements that align with the specific requirements and sensitivities of the healthcare domain. The absence of such tailored frameworks, as exemplified by the MomConnect and Kena Health initiatives, risks subjecting users to the terms and conditions of third-party service providers, creating disparities in data protection, consent mechanisms, and accountability measures. Moreover, the juxtaposition of government-regulated medical data and user-generated health data, as discussed by Kostkova et al.,[147] raises important questions about the diverse motivations and awareness levels of users engaging with digital health platforms. The suggestion that citizens may feel their explicit consent is required for data sharing in the former group, while tacitly accepting data sharing with private entities in the latter group, highlights the need for further research to understand the nuances of user perceptions and decision-making processes in this context.

The analysis has also identified knowledge gaps regarding the potential power dynamics and asymmetries inherent in the international division of labour within the digital platform ecosystem. The foreign ownership and development of platforms like Kena Health, coupled with the opacity surrounding their legal and data handling practices, raise concerns about the agency and self-determination of local communities in the development and deployment of digital health solutions.

[147] Supra, n 138

Addressing these issues is crucial for ensuring the responsible and equitable distribution of the benefits of digital health technologies, particularly in developing country settings.

Future research should delve deeper into the specific legal and regulatory frameworks governing digital health platforms, with a focus on developing country contexts. Comparative analyses of the approaches taken by different jurisdictions, as well as the examination of case studies involving successful collaborations between local communities and platform owners, could provide valuable insights to inform policymaking and best practices. Additionally, empirical studies exploring user perceptions, trust, and decision-making processes regarding the sharing of health data, across diverse demographic and cultural backgrounds, would contribute to a more nuanced understanding of the socio-legal challenges in this domain.

2.4. Conclusion

This scoping study on the digital health ecosystem in South Africa, with a particular focus on the health app landscape, has provided a multi-layered understanding of the complex challenges and opportunities presented by the rapid proliferation of these innovative technologies. Through an examination of the legislative and regulatory frameworks, the institutional governance structures, and the diverse stakeholder landscape, the study has illuminated the intricate tapestry of factors shaping the development, deployment, and adoption of health apps in the country. The analysis has underscored the critical need for a coherent and context-sensitive approach to the governance of digital health solutions, one that prioritises user rights, data sovereignty, and the equitable distribution of benefits.

A key finding of this study is the lack of a comprehensive regulatory framework specifically tailored to address the unique risks and challenges posed by health apps and mobile data collection. While South Africa's existing laws, such as the Protection of Personal Information Act (POPIA), provide a general foundation for data protection, the study has revealed significant gaps in the ability of these regulations to effectively govern the complex and rapidly evolving digital health landscape. The absence of clear guidelines on informed consent, data security, and cross-border data transfers creates uncertainties and vulnerabilities that could compromise user privacy and autonomy. Furthermore, the study has highlighted the dearth of evidence-based research evaluating the effectiveness and impact of health apps on health outcomes and healthcare delivery processes in the South African context. This knowledge gap hinders the development of informed policies and regulations, as policymakers and healthcare providers are unable to make decisions grounded in rigorous, context-specific data.

The analysis of the health app ecosystem has also exposed the intricate power dynamics and potential asymmetries inherent in the relationship between locally developed apps and those created by foreign entities. The reliance on foreign technologies and software raises concerns about data sovereignty, the alignment of these apps with local cultural and linguistic nuances, and the potential for the perpetuation of biases and exclusion. Underscoring these challenges is the overarching need to ensure transparency, user control, and the protection of individual rights in the digital health domain. The study has revealed how the complexity and opacity of terms and privacy policies often advantage app owners and data processors, leaving users vulnerable to exploitation and the erosion of their autonomy.

HFW HOUSE OF FISCAL WISDOM
بيت الحكمة المالية
NYUMBA YA HEKIMA YA FEDHA