APRIL 2025

A STUDY ON DIGITAL HEALTH APPS IN KENYA: THE CASE OF M-TIBA, ADA & LESSONS LEARNT

HFW REPORTS

Prepared By :
Lyla Latif (PhD)

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

Table of Contents

1. Introduction 2

2. Digital Health in Kenya 4

2.1. Mapping the Regulatory Environment 4
2.1.1. Strategies, Policies, Laws and Regulations 4
2.1.2. Governing Institutions 6
2.1.3. Actors 9
2.1.4. Testing Environment for Health Apps 10
2.1.5. Lessons Learnt 12

2.2. The Health Apps Ecosystem 13
2.2.1. Methods 13
2.2.2. Overview of the Digital Health Ecosystem 13
2.2.3. Categorisation of Health Apps 15
2.2.4. Techno-Legal Factors Impacting the Apps Ecosystem 18
2.2.5. Lessons Learnt 21

2.3. The Case of M-TIBA 22
2.3.1. Method of Analysis 22
2.3.2. Legal Analysis of M-TIBA's Contractual Terms and Privacy Policy 23
2.3.3. The Case of Ada: Comparative Analysis 26
2.3.4. Lessons Learned 28

2.4. Conclusion 29

1. Introduction

Digital health in Africa has been enabled by rising mobile subscriptions and internet access.[1] It encompasses the application of digital and mobile technologies to promote health, prevent disease, diagnose and monitor health issues, deliver clinical care, empower patients and advance universal health coverage across Africa.[2] It includes tools spanning mHealth, telemedicine, virtual care platforms, health management information systems, data analytics, internet of things, artificial intelligence, electronic health records, personal health tracking devices and advanced health technologies.[3] Literature also suggests digital health is progressively transforming how African communities access and perceive healthcare.[4] Onyango and Ondiek discuss how African governments scaled up digital health tools to continue service provision during lockdowns amidst the COVID-19 pandemic.[5] Miller et al. examine Rwanda's use of drones, robots and data dashboards to augment epidemic surveillance and response.[6] Ibeneme et al highlight the potential of

[1] Sezgin, E., 'Introduction to Current and Emerging mHealth Technologies: Adoption, Implementation, and Use', in E. Sezgin et al (eds), *Current and Emerging mHealth Technologies* (Springer, 2018)

[2] Ngoc CT, Bigirimana N, Muneene D., et al., 'Conclusions of the digital health hub of the Transform Africa Summit (2018): strong government leadership and public-private-partnerships are key prerequisites for sustainable scale up of digital health in Africa', *BMC Proceedings*, 12:11 (2018), 17; Tambo E, Madjou G, Mbous Y et al., 'Digital Health Implications in Health Systems in Africa', *European Journal of Pharmaceutical and Medical Research* 3:1 (2016), 91-93.

[3] Musa SM, Haruna UA, Manirambona E., et al., 'Paucity of Health Data in Africa: An Obstacle to Digital Health Implementation and Evidence Based Practice', *Public Health Reviews Policy Brief* (2023).

[4] Onyango G and Ondiek JO., 'Open innovation during the COVID-19 pandemic policy responses in South Africa and Kenya', *Politics & Policy* (2022); 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; Ibeneme S, Okeibunor J, Muneene D et al., 'Data revolution, health status transformation and the role of artificial intelligence for health and pandemic preparedness in the African context', *BMC Proceedings* 15:15 (2021), 22; Murray E, Hekler EB, Andersson G et al., 'Evaluating Digital Health Interventions: Key questions and approaches', *American Journal of Preventive Medicine* 51:5(2016), 843-851.

[5] Onyango G and Ondiek JO., 'Open innovation during the COVID-19 pandemic policy responses in South Africa and Kenya', *Politics & Policy* (2022).

[6] 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.

digital health analytics to uncover insights from health datasets that can inform planning, forecasting and interventions.[7] Murray et al scope evidence on how digital self-care interventions enhance patient empowerment and engagement across prevention and disease management while overcoming geographic barriers.[8]

Such solutions expand convenience of accessing healthcare information, education, remote consultation services, prescription deliveries, test results notification and appointment bookings.[9] Automated personal health tracking and alerts can assist prevention and self-management of chronic diseases.[10] Digital symptom checkers and medical chatbots offer basic screening or triaging support as well. Integration of payment systems into health apps enables affordable transactions. By bridging geographic and administrative barriers, digital health enhances perceptions of self-efficacy and nudges attitudinal shifts around individual responsibility for maintaining wellness or managing conditions.[11] While the significance of digital health lies in strengthening healthcare access, quality, outcomes and equity across Africa, there are also constraints that have hindered realisation of its full potential thus far.

Scholarship on digital health in Africa highlight barriers spanning infrastructural, policy, regulatory, financial, ethical and cultural spheres.[12] Core bottlenecks include unstable electricity access affecting remote regions,[13] health facility digitisation gaps,[14] connectivity issues limiting reach of interventions,[15] interoperability limitations leading to isolated data silos,[16] dependence on external donor funding models rather than domestic commitment,[17] lack of policies regarding privacy protections, consent processes and liability allocation,[18] mismatches between some technology design assumptions and community expectations,[19] and ethical issues around informed consent for personal data sharing and analysis.[20]

Additionally, regulatory gaps arise where existing legal and policy structures fail to offer clarity on oversight mechanisms, quality thresholds, security safeguards and liability allocation specifically for software-based health

[7] Ibeneme S, Okeibunor J, Muneene D et al., ‘Data revolution, health status transformation and the role of artificial intelligence for health and pandemic preparedness in the African context’, *BMC Proceedings* 15:15 (2021).

[8] Murray E, Hekler EB, Andersson G et al., ‘Evaluating Digital Health Interventions: Key questions and approaches’, *American Journal of Preventive Medicine* 51:5(2016), 843-851.

[9] 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; Murray E, Hekler EB, Andersson G et al., ‘Evaluating Digital Health Interventions: Key questions and approaches’, *American Journal of Preventive Medicine* 51:5(2016), 843-851.

[10] Ibeneme S, Okeibunor J, Muneene D et al., ‘Data revolution, health status transformation and the role of artificial intelligence for health and pandemic preparedness in the African context’, *BMC Proceedings* 15:15 (2021).

[11] Onyango G and Ondiek JO., ‘Open innovation during the COVID-19 pandemic policy responses in South Africa and Kenya’, *Politics & Policy* (2022).

[12] Townsend BA, Sihlahla I, Naidoo M., et al., ‘Mapping the regulatory landscape of AI in healthcare in Africa’, *Front. Pharmacol.* 14:1214422 (2023); Musa SM, Haruna UA, Manirambona E., et al., ‘Paucity of Health Data in Africa: An Obstacle to Digital Health Implementation and Evidence Based Practice’, *Public Health Reviews Policy Brief* (2023); Ngoc CT, Bigirimana N, Muneene D., et al., ‘Conclusions of the digital health hub of the Transform Africa Summit (2018): strong government leadership and public-private-partnerships are key prerequisites for sustainable scale up of digital health in Africa’, *BMC Proceedings*, 12:11 (2018), 17.

[13] Sezgin, E., ‘Introduction to Current and Emerging mHealth Technologies: Adoption, Implementation, and Use’, in E. Sezgin et al (eds), *Current and Emerging mHealth Technologies* (Springer, 2018).

[14] Tambo E, Madjou G, Mbous Y et al., ‘Digital Health Implications in Health Systems in Africa’, *European Journal of Pharmaceutical and Medical Research* 3:1 (2016), 91-93.

[15] van Reisen M, Oladipo F, Stokmans M., et al., ‘Design of a FAIR digital data health infrastructure in Africa for COVID-19 reporting and research’, *Advanced Genetics* (2021).

[16] Townsend BA, Sihlahla I, Naidoo M., et al., ‘Mapping the regulatory landscape of AI in healthcare in Africa’, *Front. Pharmacol.* 14:1214422 (2023).

[17] Sezgin, E., ‘Introduction to Current and Emerging mHealth Technologies: Adoption, Implementation, and Use’, in E. Sezgin et al (eds), *Current and Emerging mHealth Technologies* (Springer, 2018); Ngoc CT, Bigirimana N, Muneene D., et al., ‘Conclusions of the digital health hub of the Transform Africa Summit (2018): strong government leadership and public-private-partnerships are key prerequisites for sustainable scale up of digital health in Africa’, *BMC Proceedings*, 12:11 (2018).

[18] Townsend BA, Sihlahla I, Naidoo M., et al., ‘Mapping the regulatory landscape of AI in healthcare in Africa’, *Front. Pharmacol.* 14:1214422 (2023).

[19] Sezgin, E., ‘Introduction to Current and Emerging mHealth Technologies: Adoption, Implementation, and Use’, in E. Sezgin et al (eds), *Current and Emerging mHealth Technologies* (Springer, 2018).

[20] van Reisen M, Oladipo F, Stokmans M., et al., ‘Design of a FAIR digital data health infrastructure in Africa for COVID-19 reporting and research’, *Advanced Genetics* (2021).

technologies and algorithms in emerging areas like AI, mHealth apps and telemedicine platforms.[21] Risks also stem from widespread use of third-party software developer platforms to rapidly build health apps, where vulnerabilities in these platforms or unauthorised data access during app hosting on cloud servers can undermine protections.[22] Such deficits risk inequitable diffusion of benefits, digital exclusion of marginalised groups, and inadequate safeguards against misuse of sensitive health data.

Furthermore, the growth of digital health has seen extensive private sector interest, as gaps in health infrastructure prompt technology developers and healthcare companies to create health apps addressing unmet consumer needs. Local startups leverage investor funding while multinationals expand African operations, crafting apps spanning patient education, teleconsultation, diagnostic screening and more.[23] However, the profit incentives prompting the app boom also engender risks.[24] Zuboff explains how surveillance capitalism enables powerful technology interests to gain asymmetrical advantages through monetising user data extracted from smart digital platforms. In the health context, extensive behavioural tracking by apps could enable unauthorised marketing, profiling, and exploitative targeting based on sensitive medical data rather than primarily serving user welfare. Couldry and Mejias further caution that the logics of digitalisation tend towards converting human experience into extractable data assets, prioritising accumulation imperatives over social rights.[25] Health apps may illustrate risks of such data colonialism where intimate illness revelations become conduits for optimising visibility and microtargeting health system users rather than respecting care duties.

Given the potential of digital health to transform healthcare access and also understanding the risks it poses, this study undertakes an in-depth analysis of the digital health regulatory environment and ecosystems in Kenya, South Africa and Uganda. The scoping analysis will focus on:

a. Mapping the regulatory environment encompassing laws, regulations, policies and government strategies enacted around digital health and the actors involved.

b. Studying the emergence, growth and use of the health app ecosystem, analysing developmental factors including financing and funding flows, target user segments, adoption patterns, functionality and categorisation of the health apps. An examination of interdependencies of health apps with digital payment platforms and mobile banking showing how online consultation, e-prescriptions, payments, health records are all connected.

c. Reviewing and evaluating widely used apps that are locally developed and those that are foreign. Their examination will explore their infrastructure ownership, consent flows and platform gatekeeper accountabilities. This is done to understand whether the apps uphold capital interests subordinating welfare. An examination of the terms of service, privacy policies and consumer protections provisions will also be made to identify any surveillance and security risks.

2. Digital Health in Kenya

2.1. Mapping the Regulatory Environment

2.1.1. Strategies, Policies, Laws and Regulations

The landscape of digital health in Kenya, as it stands today, is a rich tapestry interwoven with constitutional mandates, legislative frameworks, policy blueprints, and the evolving roles of various regulatory bodies. This ecosystem

[21] Townsend BA, Sihlahla I, Naidoo M., et al., 'Mapping the regulatory landscape of AI in healthcare in Africa', *Front. Pharmacol.* 14:1214422 (2023); Ngoc CT, Bigirimana N, Muneene D., et al., 'Conclusions of the digital health hub of the Transform Africa Summit (2018): strong government leadership and public-private-partnerships are key prerequisites for sustainable scale up of digital health in Africa', *BMC Proceedings*, 12:11 (2018); Tambo E, Madjou G, Mbous Y et al., 'Digital Health Implications in Health Systems in Africa', *European Journal of Pharmaceutical and Medical Research* 3:1 (2016), 91-93.

[22] Musa SM, Haruna UA, Manirambona E., et al., 'Paucity of Health Data in Africa: An Obstacle to Digital Health Implementation and Evidence Based Practice', *Public Health Reviews Policy Brief* (2023).

[23] Al Dahdah M., 'Digital markets and the commercialisation of healthcare in Africa: the case of Kenya', *Globalisations* (2022).

[24] Zuboff, S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).

[25] Couldry, N., & Mejias, U. A. *The Costs of Connection*: *How Data is Colonizing Human Life and Appropriating It for Capitalism* (Stanford University Press, 2019).

is not just a set of independent elements but a cohesive structure that aims to address the complexities and challenges of integrating technology into healthcare.

Kenya's growth towards digital health lies in the 2010 Constitution.[26] Although the Constitution does not explicitly mention digital health, it lays down the normative foundations for this domain. The Constitution recognises health as a fundamental right under Article 43(1)(a), embedding values like human dignity, equity, social justice, inclusiveness, equality, and non-discrimination. These values are crucial in governing technologies that impact human well-being. Scholars like Brownsword[27] and Hilderbrandt[28] have emphasised the importance of incorporating these constitutional values into the design and oversight of algorithmic systems. They argue that such integration is more effective in upholding rights in emerging techno-social contexts than relying solely on subsequent regulation, which often leads to narrow bureaucratic compliance. The pervasive nature of digital infrastructure in Kenya, from connectivity backbones to mobile platforms, places it squarely within the realm of public utility services, thereby necessitating accountability akin to that governing water, healthcare, or roads.

In terms of strategic policy, the Ministry of Health's Kenya eHealth Strategy 2011-2017[29] and Kenya Health Policy 2014-2030[30] explicitly commits to harnessing technology for quality healthcare delivery. This strategy and policy are further supported by the National eHealth Policy 2016-2030,[31] which outlines a comprehensive technology adoption roadmap, including shared health records, data exchange standards, cybersecurity, and national patient identifiers. The strategy underscores the balance between innovation and ethical safeguards, emphasising privacy, security, and building a sustainable technical workforce. Parallel to health-specific strategies, the Ministry of Information, Communications and the Digital Economy's National ICT Masterplan[32], the Digital Economy Blueprint[33], and the Kenya National Digital Master Plan 2022-2032[34] have focused on broader aspects such as e-Government services, infrastructure upgrades, and promoting digital adoption across various sectors, including health. Programs like the integrated Huduma[35] public service delivery system based on its Huduma Kenya Digitalization Plan 2023/2024-2025/2026 are operationalising many digital initiatives, directly impacting healthcare delivery through aspects like payments integration, automation, and digital record-keeping.[36]

In the realm of legislation, several recent laws have furthered the cause of digital health. The Health Act 2017[37] recognises eHealth and telemedicine as legitimate mediums for healthcare delivery. It mandates the maintenance of accurate health records and the implementation of security safeguards, establishing a rights-based framework for digital health platforms. The Computer Misuse and Cybercrimes Act 2018[38] and the Data Protection Act 2019[39] provide additional layers of legal protection, covering aspects like unauthorised system access, data privacy, and consent. However, the effectiveness and scope of these laws in dealing with the nuances of digital health, especially algorithmic complexities, are subjects of ongoing debate.

In the regulatory landscape of healthcare in Kenya, several legislative frameworks complement the Medical Practitioners and Dentists Act[40] and the Nurses and Midwives Act,[41] collectively shaping the governance of healthcare

[26] Government of Kenya, 'Constitution of Kenya, 2010' (Nairobi: National Council of Law Reporting).
[27] Brownsword, R. (2019). Law, Technology and Society: Reimagining the Regulatory Environment. Routledge.
[28] Hildebrandt, M. (2015). Smart technologies and the end(s) of law: Novel entanglements of law and technology. Edward Elgar Publishing.
[29] Government of Kenya, Ministry of Health, 'Kenya eHealth Strategy 2011-2017' (Nairobi: Government Printers).
[30] Government of Kenya, Ministry of Health, 'Kenya Health Policy 2014-2030' (Nairobi: Government Printers).
[31] Government of Kenya, Ministry of Health, 'Kenya National eHealth Policy 2016-2030' (Nairobi: Government Printers).
[32] Republic of Kenya, ICT Authority, The Kenya National ICT Master Plan 2013/14 – 2017/18 (Nairobi: Government Printers, 2014); http://196.207.23.2:8080/handle/123456789/66
[33] Republic of Kenya, Digital Economy Blueprint: Powering Kenya's Transformation (Nairobi: Government Printers, 2019).
[34] Republic of Kenya, Ministry of ICT, Innovation and Youth Affairs, The Kenya National Digital Master Plan 2022-2032 (Nairobi: Government Printers, 2022).
[35] https://www.hudumakenya.go.ke/services
[36] Republic of Kenya, Ministry of Public Service, Gender and Affirmative Action, Huduma Kenya Digitalisation Plan 2023/2024-2025/2026 (Nairobi: Government Printers, 2023).
[37] Government of Kenya, 'Health Act, No 21 of 2017' (Nairobi: National Council of Law Reporting).
[38] Government of Kenya, 'Computer Misuse and Cybercrimes Act No 5 of 2018' (Nairobi: National Council of Law Reporting).
[39] Government of Kenya, 'Data Protection, No 24 of 2019' (Nairobi: National Council of Law Reporting).
[40] Government of Kenya, 'Medical Practitioners and Dentists Act, Cap 253' (Nairobi: National Council of Law Reporting).
[41] Government of Kenya, 'Nurses and Midwives Act, Cap 257' (Nairobi: National Council of Law Reporting).

practitioners. The Clinical Officers (Training, Registration and Licensing) Act, 2017[42] for instance, oversees the training, registration, and licensing of clinical officers, who are integral to healthcare provision in Kenya. This act also touches upon eHealth aspects pertinent to clinical officers. The Pharmacy and Poisons Act[43] plays a crucial role in controlling the pharmaceutical sector, regulating the practices of pharmacists and overseeing the management of pharmaceutical products and medical substances.

Additionally, the Public Health Act,[44] while not directly focused on healthcare practitioners, is pivotal for managing public health, encompassing the prevention of communicable diseases and maintaining sanitation and general public health welfare. The Kenya Medical Supplies Authority Act, 2013[45] though more aligned with logistics and supply chain management, indirectly influences healthcare practitioners by ensuring the availability of essential medical supplies. The Mental Health Act[46] is another key piece of legislation, specifically targeting the regulation of mental health care providers and services. It sets out guidelines for the treatment and care of individuals with mental health conditions, as well as standards for mental health facilities. Moreover, the Health Records and Information Managers Act,[47] while not directly regulating healthcare practitioners, is crucial for the management of health records, a vital component in the era of digital health.

However, when we pivot to the domain of digital health technologies—particularly the development of health apps and digital interventions—there is a conspicuous regulatory vacuum. The existing legal instruments, such as the Computer Misuse and Cybercrimes Act, offer a framework for addressing certain aspects of digital health, like cybersecurity and data privacy. Nevertheless, these laws primarily focus on penalising misconduct after it occurs rather than setting out preventative guidelines or standards for the development process. As such, developers of digital health apps operate in a space that lacks the stringent oversight applied to traditional healthcare providers. The Data Protection Act of Kenya stands as a critical legal framework for safeguarding personal data in the digital age, particularly within the realm of health apps that handle sensitive user information. While it establishes the requirement for user consent in tracking and data processing, its efficacy is challenged when dealing with foreign app providers operating outside the jurisdiction of Kenyan law. These complexities are magnified by the intricate network of third-party agreements that underpin app functionality, posing significant hurdles for local enforcement.

The intricate network of third-party agreements refers to the contracts and understandings that app developers have with other service providers, such as cloud hosting platforms, analytics services, and advertising networks. These agreements are essential for the apps' operations, as they can provide necessary infrastructure, data analysis, and monetisation models. However, because these third parties often operate in different jurisdictions with varying legal standards, it can be difficult for a single country's laws, like those in Kenya, to exert authority over them. Therefore, given the international nature of data flow and the operation of digital health technologies, the Data Protection Act's reach is tested. This gap in regulation can have significant implications. Without proper oversight, there is a risk that digital health technologies may not align with the high standards of patient safety, privacy, and efficacy that are demanded in other areas of healthcare.

2.1.2. Governing Institutions

Continuing from the regulatory framework, the institutional landscape in Kenya involved in digital health is both diverse and dynamic, encompassing various government ministries, regulatory bodies, and specialised agencies. At the forefront is the Ministry of Health,[48] which plays a central role in shaping and implementing Kenya’s health policies, including those related to digital health. This ministry is responsible for the overarching strategic direction of health services in the country and works closely with other government entities to integrate digital technologies into healthcare delivery. The Ministry of Health's involvement extends from policy formulation, such as the Kenya Health Policy 2014-2030, to overseeing the implementation of specific digital health initiatives. In tandem, the Ministry of

[42] Government of Kenya, ‘Clinical Officers (Training, Registration and Licensing) Act No 20 of 2017’ (Nairobi: National Council of Law Reporting).
[43] Government of Kenya, ‘Pharmacy and Poisons Act, Cap 244’ (Nairobi: National Council of Law Reporting).
[44] Government of Kenya, ‘Public Health Act, Cap 242’ (Nairobi: National Council of Law Reporting).
[45] Government of Kenya, ‘Kenya Medical Supplies Authority Act No 20 of 2013’ (Nairobi: National Council of Law Reporting).
[46] Government of Kenya, ‘Mental Health Act, Cap 248’ (Nairobi: National Council of Law Reporting).
[47] Government of Kenya, ‘Health Records and Information Managers Act, No 15 of 2016’ (Nairobi: National Council of Law Reporting).
[48] https://www.health.go.ke/

Information, Communications, and the Digital Economy (ICDE)[49] is a key player, especially in areas concerning the technological infrastructure required for digital health. This ministry's responsibilities include the development of the national ICT infrastructure, which is crucial for enabling digital health services, particularly in remote and rural areas. The Ministry of ICDE also collaborates with the Ministry of Health in developing policies and strategies that leverage technology for health services, as seen in initiatives like the National eHealth Strategy.

Another important institution is the Kenya Medical Supplies Authority (KEMSA),[50] which, while primarily focused on medical logistics and supply chain management, is increasingly involved in digital solutions for inventory management and distribution of medical supplies. This aspect is critical for ensuring that healthcare facilities are well-equipped and that medical supplies are efficiently managed and distributed. The Pharmacy and Poisons Board,[51] under the Ministry of Health, is responsible for regulating pharmaceuticals and medical devices, including digital health apps classified as medical devices. This board's role in certifying and overseeing digital health tools is becoming increasingly vital as more such technologies enter the Kenyan healthcare market. Moreover, regulatory bodies such as the Medical Practitioners and Dentists Board[52] and the Nursing Council of Kenya,[53] while traditionally focused on regulating healthcare professionals, are also increasingly involved in aspects of digital health. These bodies are adapting their regulatory frameworks to include standards and guidelines for the use of digital technologies in medical and nursing practices.

Furthermore, the National Hospital Insurance Fund (NHIF)[54] plays a role in the digital health ecosystem, particularly in terms of financing healthcare services and integrating digital solutions for claims processing and member management. The involvement of NHIF in digital health is key to ensuring that these technologies are accessible and affordable for the broader population. The Communications Authority of Kenya (CA)[55] also plays a pivotal role. As the regulatory authority for the communications sector, the CA ensures the availability of quality communication services throughout the country, including those necessary for digital health interventions. With the burgeoning of e-health services, the CA's oversight on data transmission and internet services becomes increasingly critical.

The Office of the Data Protection Commissioner[56] is another key institution, tasked with the enforcement of the Data Protection Act. This office's mandate is to safeguard personal data by regulating the processing of personal information, a function that directly impacts digital health platforms that handle sensitive health data. Additionally, the Judiciary[57] in Kenya has a role in the digital health ecosystem, as it interprets the laws and adjudicates cases involving digital health matters. It is the ultimate arbiter when there are disputes or challenges regarding the application of digital health regulations, data protection, and the rights of citizens as they intersect with digital health services. While Kenya moves towards healthcare innovation expanding access by leveraging on digitalisation, critics argue the pace of transformation risks outpacing policy evolution. Core apprehensions centre on the capacity of existing legal instruments and oversight bodies regulating traditional facility-based care to transplant into software-mediated treatment realms with heightened consent complexity and data exploitation risks.[58]

At the crux lies concerns around healthcare data stewardship, as apps and algorithmic systems gain mediated agency through intimate health histories input for functionality.[59] As Zuboff elucidates, the logics of ‘surveillance capitalism’[60] enable platform owners to instrumentalise captured experiences into monetised data derivatives. In healthcare, these risks appropriating illness narratives as adhesive assets for optimisation—rather than respecting legally

[49] https://ict.go.ke/

[50] https://www.kemsa.go.ke/

[51] https://web.pharmacyboardkenya.org/

[52] https://kmpdc.go.ke/

[53] https://nckenya.com/

[54] https://www.nhif.or.ke/

[55] https://www.ca.go.ke/

[56] https://www.odpc.go.ke/

[57] https://judiciary.go.ke/

[58] Townsend BA, Sihlahla I, Naidoo M, et al., ‘Mapping the regulatory landscape of AI in healthcare in Africa’, *Front. Pharmacol.* 14:1214422 (2023).

[59] Ministry of Information, Communication and the Digital Economy, ‘Sectoral Working Group Report on Emerging Technologies and Data Governance, December 2023’.

[60] Zuboff, S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).

enshrined care duties. Similarly, Couldry & Mejias highlight risks of 'data colonialism'[61] where life becomes reduced to mineable breadcrumbs rather than the locus of welfare rights. Thus, scholars emphasise that before diffusing digital public goods, policy must consciously parse new accountability channels on organisations gaining visibility from health data trails frequently beyond direct patient comprehension or control.[62]

However, despite bold blueprints like the National eHealth Policy 2016-2023 identifying such technology adoption complexities, existing capacity deficits constrain swift realisation of ethical, secure innovation pathways called for. As outlined earlier, healthcare oversight presently relies on bodies like the Kenya Medical and Dentist Board regulating individual practitioners rather than systems gained mediated agency through patient data. The Pharmacy and Poisons Board oversees medical devices and drugs—but apps bypass such frameworks until explicitly re-categorised despite acting on sensitive diagnoses and biomarkers. The Health Records and Information Managers Board focuses largely on paper-based patient management rather than data lakes accumulating digital trails. While NHIF is expanding coverage and piloting digitally integrated financing for care access, its oversight concentrates on accreditation and reimbursement processes rather than tracing onward information flows to third parties.

The Office of the Data Protection Commissioner established under recent legislation does mandate consent, processing protocols and protection requirements for personal data including medical history sensitivity. However, critics highlight gaps in practical enforcement capacity over diverse health sector players, from insurers to hospitals and apps—each requiring customised sectoral guidance for compliance rather than reliance on individual complaint investigation alone to demonstrate efficacy.[63] Moreover the law inherently struggles regulating foreign app developers outside local jurisdictional control[64] despite accumulating records on Kenyan citizen usage.

Such limitations catalyse calls for an expanded policy remit envisioning healthcare oversight as stewardship over sociotechnical systems. As apps reshape health data flows between patients, platform owners, third party suppliers, insurers and the state—accountability requires examining consent, ethics and welfare across entire stacks collectively impacting healthcare experiences. Beyond practitioners, this necessitates oversight on software vendors, device manufacturers, data processors and AI providers integral to digital health ecosystems with frequently misaligned incentive priorities relative to public care duties.[65]

While Kenya has progressive eHealth strategy vision explicitly seeking such balanced innovation, I argue that goodwill alone cannot outpace risks from accelerated growth of digital health interventions such as health apps bereft of robust impact evaluation or rights safeguards emerging from commercial proprietary systems tethered more to profit sustainability rather than health equity principles. Recent partnerships, for example, between Kenya's Safaricom and Dutch consortium PharmAccess[66] in launching M-TIBA, a health wallet, highlight these tensions—where reliance on proprietary backends beyond patient control persists despite policy pledges otherwise (I discuss this later in section 2.3.). The scenario underscores need for governance reinvention through cooperation advancing structural rights across evolving health platforms rather than assuming voluntary self-regulation reliably aligns private interests with social welfare.[67]

Beyond the government-led regulatory framework, the Kenyan digital health space is enriched by the active participation of non-governmental organisations, private entities, and international collaborators. These stakeholders are integral to the diverse initiatives that drive the digital health sector forward. Central to these initiatives are health apps,

[61] Couldry, N., & Mejias, U. A. *The Costs of Connection*: *How Data is Colonizing Human Life and Appropriating It for Capitalism* (Stanford University Press, 2019).

[62] van Dijck, Poell, T., and de Waal, M*., The Platform Society: Public Values in a Connective World* (Oxford University Press, 2018).

[63] Mutua, S and Yanqiu, Z., 'Online content regulation policy in Kenya: potential challenges and possible solutions', *Journal of Cyber Policy* Vol 6, Issue 2 (2021); Ndung'u, N., 'Digital Technology and State Capacity in Kenya' CGD Policy Paper 154 (2019) Washington, DC.

[64] Coleman, D., 'Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws' *Michigan Journal of Race and Law* 422 (2019)

[65] Cowls, J., Morley, J and Floridi, L., 'App store governance: Implications, limitations, and regulatory responses', *Telecommunications Policy*, Vol 47, Issue 1 (2023); Perez-Pozuelo, I., Spathis, D., Gifford-Moore, J et al., 'Digital phenotyping and sensitive health data: Implications for data governance', *Journal of the American Medical Informatics Association*, Vol 28, Issue 9 (2021); 2002-2008

[66] https://www.pharmaccess.org/who-we-are/

[67] Townsend BA, Sihlahla I, Naidoo M, et al., 'Mapping the regulatory landscape of AI in healthcare in Africa', *Front. Pharmacol.* 14:1214422 (2023).

which represent a significant intersection of technology and healthcare. These apps are a focal point for various actors in the digital health arena, signifying a shift in how healthcare services are accessed and delivered.

2.1.3. Actors

Kenya's digital health ecosystem involves diverse collaborations between state and non-state actors spanning regulatory agencies, development partners, private companies, healthcare providers, academia and non-governmental organisations. These multi-stakeholder engagements unite complementary capabilities tackling stubborn challenges across health system building blocks from financing, and infrastructure to workforce and access. Notable government stewards include the Ministry of Health framing national e-health vision and policy, ICT Authority developing digital infrastructure, and Kenya National Bureau of Statistics[68] leveraging data analytics for responsive planning.[69] Beyond policymaking, governmental insurers like NHIF integrate systems reaching national scale for universal care. Parastatal regulators like NACOSTI[70] ensure ethical orientation aligns innovation to public goods.

Philanthropies like PharmAccess also play a role in the digital health space in Kenya by assessing the viability, effectiveness, and potential impact of new healthcare ideas and technologies. This involves evaluating the feasibility and effectiveness of solutions, ensuring they address specific health needs effectively and are adaptable to local contexts. The importance of such validation is particularly highlighted in the context of startups that might possess innovative ideas but lack the resources or expertise for comprehensive testing and refinement.[71] Technology giants like Intel and Microsoft offer global best practices while telcos like Safaricom provide identity/payment rails streamlining scale for digital platforms.

Private insurers and providers like UAP insurance[72] and Minet Kenya[73] build digital infrastructure expanding consumer choice at market-driven efficiencies. Government partnerships integrate such solutions within national policy goals around healthcare access and equity. In this case, Safaricom and PharmAccess have collaborated with the National Hospital Insurance Fund (NHIF) to operate the M-TIBA platform, which is a mobile health wallet, that enables users to save, send, and receive funds specifically for healthcare services.[74] This partnership aligns with Kenya's national goals to enhance access to healthcare services and promote equity by leveraging digital platforms and mobile technology to reach a broader segment of the population, including those in remote areas. An important aspect of this system is the management of the funds stored within M-TIBA. UAP Insurance, known for its insurance products and services, is responsible for managing these funds.[75] This involvement of UAP Insurance ensures that the funds are handled with the same rigour and security as traditional insurance products, providing users with confidence in the safety and integrity of their healthcare savings. The role of UAP Insurance in managing M-TIBA funds underscores the collaborative nature of the digital health ecosystem, where different entities bring their expertise to support the overarching goal of improved healthcare access and financial management for healthcare needs in Kenya.

Think tanks like the Kenya Medical Research Institute (KEMRI) generate evidence guiding appropriate innovation in health.[76] Universities also offer crucial R&D, prototyping and talent development around ethical, secure digital public goods.[77] Social enterprises also play a role in the digital health space. They tailor health models to fit the unique demands of local communities, guided by the principle of user centric design.[78] This approach emphasises the creation of digital health solutions that are not only innovative but also deeply rooted in the specific needs and behaviour

[68] https://www.knbs.or.ke/

[69] Moturi, C., and Gathuru, W., 'Big Data adoption in official statistics in Kenya: Challenges, opportunities and determinants', *Statistical Journal of the IAOS*, Vol 38, No. 1 (2022); 252-262

[70] https://www.nacosti.go.ke/

[71] de Wit, T., Janssens, W., Antwi, M et al., 'Digital health systems strengthening in Africa for rapid response to COVID19', *Front Health Serv*, 28:2 (2022)

[72] https://lifecareinternational.com/uap-insurance/

[73] https://www.minet.com/kenya/

[74] Neumark T and Prince R J., 'Digital Health in East Africa: Innovation, Experimentation and the Market', *Global Policy* volume 12, supp 6 (2021).

[75] https://www.cgap.org/blog/digital-platform-to-manage-out-of-pocket-health-care-expenses

[76] KEMRI, 'Ethics of Electronic Health Research', KEMRI Bioethics Review, Vol iii, Issue IV (2013).

[77] University of Nairobi, Centre for Health Informatics and Digital Health, https://chidh.uonbi.ac.ke/

[78] Holst, C, Sukums, F, Radovanovic, D., et al., 'Sub-Saharan Africa – the new breeding ground for global digital health', *The Lancet Digital Health*, Vol 2, Issue 4, E160-E162 (2020).

of the end users. Additionally, international development partners like USAID provide advisory support, project funding, South-South partnerships and implementation insights accumulated from global deployments. UN agencies share normative frameworks balancing innovation risks, while WHO endorses health data standards enabling valuable analytics. Beyond development cooperation, medical equipment multinationals are entering local partnerships expanding diagnostics access leveraging connectivity. Pharmaceutical majors are also piloting digital platforms such as Zuri Health[79] and My Dawa[80] in addition to M-Tiba connecting authenticated patients to verified providers for ethical off-label medicine access, tackling prohibitive costs.

The collaboration between the philanthropies, private sector and the government in healthcare reflects an evolution in state responsibility under the right to health and the duty to respect, protect, and fulfil health services, delivered in conjunction with private sector players. This convergence hints at a reimagined approach where the right to health is no longer a purely governmental responsibility. Rather, state duties to respect, protect and fulfil healthcare access manifest through partnerships with regulated private sector players offering innovation aligned with public welfare aims. While this tripartite relationship has a welfare aim associated with it, aimed at enhancing healthcare access and equity, as seen in the operation of the M-TIBA platform by Safaricom, PharmAccess, and NHIF, it also brings to the fore potential challenges, particularly the commercialisation of health by the private sector involved.[81]

Toebes explains that commercialisation of public healthcare services, which is becoming increasingly common across the world, has implications for healthcare from a human rights perspective.[82] She argues that human rights law typically does not interfere with the choice of whether health and other public services are publicly or privately provided, however, commercialisation of healthcare services can lead to a shift away from government control over the provision of services. This according to Sanders et al can potentially result in a loss of legal accountability.[83] As private providers' profit motives may push them to develop health apps aiming for financial returns rather than realising rights, they may engage in practices like extensive user tracking, profiling and arbitrary third-party data sharing without adequate consent safeguards or purpose limitations. Thus, reliance on private sector apps risks accountability gaps over upholding legal duties to right to health provisions including equitable access, welfare prioritisation and health information sovereignty. The literature on digital health in Kenya that has been covered in this scoping study does not cover any analysis of these risks by specifically focusing on the functionality of a health app used locally.

2.1.4. Testing Environment for Health Apps

Kenya has made significant progress in adopting digital health technologies to expand healthcare access, as envisioned under the National eHealth Policy 2016-2030. However, the rapid pace of digital innovation risks outstripping policy and regulatory evolution, leaving critical gaps in oversight and accountability. This is clearly evidenced in the growth of health apps and digital interventions operating without stringent regulations or testing protocols akin to those governing traditional medical providers. In the earlier sections I have discussed that the existing legal framework centred on the Computer Misuse and Cybercrimes Act, 2018 and the Data Protection Act, 2019 focuses more on penalising misconduct post-facto rather than outlining ex-ante standards or preventative safeguards. Having scrutinised the Capital Markets Authority[84] and Ministry of Health's[85] websites alongside literature[86] on regulatory sandboxes in Kenya that is mainly focused around fintech I find that there is no mandate for controlled testing of health apps to identify and mitigate risks to user safety and privacy before full-scale public deployment. This lack of regulatory sandboxes enables potentially unsafe or unethical apps to directly access the market absent oversight, raising significant legal, ethical and rights concerns.

[79] https://disruptafrica.com/2021/01/14/kenyan-startup-launches-m-health-app-to-ease-access-to-healthcare-professionals/

[80] https://africahealthitnews.com/kenya-mydawa-sceures-funding-to-become-an-all-in-one-health-platform-for-users/

[81] Al Dahdah M., 'Digital markets and the commercialisation of healthcare in Africa: the case of Kenya', *Globalisations* (2022).

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

[83] Sanders, D., De Ceukelaire, W and Hutton, B., *The Struggle for Health* (Oxford University Press, 2023).

[84] https://www.cma.or.ke/

[85] https://www.health.go.ke/

[86] Musamali, R., Jugurnath, B and Maalu, J., 'Fintech in Kenya: A policy and regulatory perspective', *Journal of Smart Economic Growth*, Vol 8, No. 1 (2023); Lubinga, S., Nhede, N T, Mangai, M et al., 'Agile governance for the 'new normal': Is Africa read?', *African Journal of Governance and Development*, Vol 11, Issue 2 (2022); Ndung'u, N., 'Digital Technology and State Capacity in Kenya', CGD Policy Paper 154 (2019).

Allowing health apps to proliferate sans gatekeeping tests or impact evaluation studies exposes consumers to diverse risks spanning from efficacy uncertainty to exploitative surveillance, given the sector's nascence.[87] While the Data Protection Act, 2019 does articulate valuable consent and processing stipulations, its enforcement reach remains restricted given jurisdictional limitations over foreign entities and practical capacity constraints in investigating every malpractice downstream. Thus, despite decent policy vision, actual impact necessitates reinforcing accountability across entire health data architectures beyond just individual point complaints. In essence, the combination of efficacy uncertainty and consent complexity in emerging app ecosystems underscores need for standardised validation mechanisms and stricter data stewardship. However, the regulatory vacuum in mandating such across digital platforms imply user welfare is left contingent on voluntary self-regulation. Expecting newly launched startups seeking returns on innovation to reliably self-impose oversight costs and utilisation barriers is optimistic unless structural incentives realign stakeholder motivations with social duties through external institutions.

I posit that given the ethical quandaries proliferating in Kenya's rapidly evolving health app landscape, there is a strong case to institute regulatory sandboxes for controlled testing of digital interventions prior to mass deployment. By allowing evidence-based investigation of risks that emerge from use of health apps from privacy, consent to interoperability within supervised settings, sandboxes can balance innovation aspirations with appropriate safeguards. There is evidence given by Leckenby et al that sandboxes are already being used for understanding the regulation of digital health interventions but this is happening in high income jurisdictions such as the global north.[88]

The utility of such steps in getting towards a sandbox for health apps is clearly validated by the successful oversight of the M-Pesa sandbox in shielding consumers while delivering trailblazing progress in digital financial access. M-Pesa's controlled experimentation approach allowed regulators to dynamically assess and mitigate emerging risks based on transparent evaluations tailored to the local context.[89] In the health app context, regulatory sandboxes can similarly require sharing masked testing data with oversight bodies to gauge efficacy and diagnostic soundness using established clinical standards before approving full operations. Approval post-trials would also mandate binding security, privacy and accountability commitments preventing misuse of captured information while enabling redress pathways. Minimum consent and data processing transparency requirements could also be instituted for consumer protection and retaining agency.

The proposal to institute pre-market sandboxes aligns with Kenya's National eHealth Policy 2016-2030 and the Digital Master Plan 2022-2032 vision itself calling for governance reinvention to match sectoral transformation and setting up of an emerging technologies sandbox alongside innovation hubs. Merely relying on existing practitioner-centric medical oversight bodies or privacy regulations centred on individual complaints is insufficient and reactive given apps reshape health data flows themselves. Failing to mandate ex-ante standards risks reduces welfare for citizens and erodes health rights in favour of platform owners seeking data commodification, surveillance optimisation and vendor lock-in effects.[90]

This section has covered the regulatory landscape, key actors, and risks around commercialisation in Kenya's digital health space. Having identified challenges like accountability gaps, health information vulnerability and oversight limitations, the next section turns to a deeper scoping of the health apps ecosystem itself. This encompasses studying the emergence, growth and use of health apps, analysing developmental factors such as financing flows, target user segments, adoption patterns across geographies and clinical categories, functionality diversity, and categorisation taxonomy. The examination also elucidates interdependencies with digital payments and mobile banking, showing how online consultation, e-prescriptions, health expenditures, and records accumulate into interconnected platforms mediating healthcare access in Kenya.

[87] Iwaya, L., Babar, A, Rashid, A et al., 'On the privacy of mental health apps', Empir Softw Eng, 28:1 (2023); Tangari, G, Ikram, M and Kaafar, M A., 'Mobile health and privacy: cross sectional study,' BMJ (2021).

[88] Leckenby, E, Dawoud, D, Bouvy, J et al., 'The Sandbox Approach and its Potential for Use in Health Technology Assessment: A Literature Review', *Applied Health Economics and Health Policy* 19 (2021): 857-869.

[89] Musamali, R., Jugurnath, B and Maalu, J., 'Fintech in Kenya: A policy and regulatory perspective', *Journal of Smart Economic Growth*, Vol 8, No. 1 (2023).

[90] Schleifer, D., 'The ecosystem trap: Why app stores perpetuate vendor lock-in' *Waterstechnology* 13 March 2023, https://www.waterstechnology.com/emerging-technologies/7950697/the-ecosystem-trap-why-app-stores-perpetuate-vendor-lock-in; Juno Health, 'Breaking Free from Vendor Lock-In: How EHR Personalisation Empowers Healthcare Independence', 14 Nov 2023, https://www.junohealth.com/blog/how-ehr-personalization-prevents-vendor-lock-in#:~:text=Vendor%20Lock%2DIn%20in%20Healthcare%20Technology&text=Vendor%20lock%2Din%20is%20similar,a%20financial%20or%20productivity%20burden.

2.1.5. Lessons Learnt

This section on mapping the regulatory environment in which digital health operates reveals several knowledge gaps. Firstly, there is limited research on the actual efficacy, quality and safety of specific health apps and digital platforms in the Kenyan context. Secondly, consumer perspectives evaluating digital health experiences requiring their intimate partnership through detailed personal data access remain conspicuously absent from existing literature. Whether citizens across literacy spectrums comprehend opaque terms-of-service agreements, or retain ongoing consent agency as backend architectures shift, necessitate careful investigation given profound power imbalances. Understanding sociocultural heterogeneity and associated variances in user comprehension of consent complexity in algorithmic systems is key.

Thirdly, while Kenya's eHealth policy ecosystem has progressive ambitions, actual accountability mechanisms governing complex data flows between patients, multitude of third-party suppliers, platform owners, and the state remain ambiguous. Beyond individual oversight bodies, enforcing structural standards on diverse apps, devices, stacks collectively impacting healthcare access requires further policy scaffolding. Moreover, practical capacity for continuous monitoring and swift intervention across dynamically evolving architectures persist as key bottlenecks. Fourthly, evidence tracing specific instances of personal health data exploitation, privacy infringements and surveillance risks is required to assess efficacy of existing regulations in Kenya beyond theoretical vulnerabilities. Studying empirical cases where algorithmic inferences or third-party partnerships compromised welfare is crucial for catalysing regulatory evolution. Similarly, instances of apps lacking interoperability or portability also need documentation given data silos erected can undermine user agency. Fifthly, evidence studying the impact of accelerating public-private convergence in health access mediation is scarce in Kenya. As apps and digitised financing diffuse, ramifications for the state’s duty to respect, protect and fulfil the fundamental right to health begs analysis given commercialisation risks and human rights law limitations on delegated obligations.

Beyond knowledge gaps, conceptual clarification around key terms is also essential. A core aspect warranting elucidation is meaningful consent, which underpins data protection. Consent implies informing users about risks, alternatives and rights regarding data use. However, lengthy impenetrable agreements listing vague possibilities strain comprehension boundaries, eroding informed voluntary participation.

Legal definitions must evolve to demand designers simplify and illustrate complex trade-offs for retaining individual dignity and control. There is no literature discussing this from the Kenyan context. Moreover, interoperability standards for data portability between apps using varying proprietary formats need elaboration within policy for preventing vendor lock-in and dependence given patients lack bargaining power relative to platforms. Similarly, the meaning of data protection itself deserves clarity, covering protection from appropriation without consent and encompassing shields against continual data referencing as machine learning models update themselves.

Areas requiring legal reform have also been identified. At the heart of Kenya’s digital health landscape lies the constitutional and legislative foundations that, although not explicitly addressing digital health, establish fundamental rights impacting this domain. Key legislations such as the Health Act 2017, the Computer Misuse and Cybercrimes Act 2018, and the Data Protection Act 2019 have set a legal framework for eHealth and telemedicine, emphasising data privacy and security. However, these laws face challenges in adequately addressing the complexities of digital health and health apps, particularly in terms of algorithmic decision-making and data stewardship.

Strategic policies and plans such as the Kenya eHealth Strategy, Kenya Health Policy, and National eHealth Policy reflect the government's commitment to integrating technology in healthcare. These policies are focused on innovation, ethical safeguards, and building a sustainable technical workforce. Despite these ambitions, there remains a significant gap between policy aspirations and practical implementation, especially in overseeing health apps and digital interventions.

The institutional framework in Kenya’s digital health sphere involves various government ministries and agencies. The Ministry of Health and the Ministry of Information, Communications, and the Digital Economy are pivotal in shaping digital health policies. Other key institutions include the Kenya Medical Supplies Authority (KEMSA), the Pharmacy and Poisons Board, and the National Hospital Insurance Fund (NHIF), each playing a role in the digital transformation of healthcare services. Traditional healthcare regulatory bodies, such as the Medical Practitioners and

Dentists Board and the Nursing Council of Kenya, are adapting to include digital health technologies. However, there is a pressing need for expanded oversight that encompasses the entire digital health ecosystem, including software vendors, data processors, and AI providers, not the existing fragmented approach.

Finally, there is a conspicuous gap in the regulation and standardisation of health apps in Kenya. Existing laws focus more on penalising misconduct than setting preventative guidelines or standards for app development. This lack of regulation exposes users to risks related to privacy, efficacy, and ethical concerns. The establishment of regulatory sandboxes for controlled testing of digital health interventions is crucial. This approach would allow for a balanced assessment of risks and benefits, ensuring user safety and privacy while fostering innovation.

2.2. The Health Apps Ecosystem

2.2.1. Methods

In studying the health app ecosystem in Kenya, purposive sampling was employed to select a representative set of health apps popular within the Kenyan context. This sampling method was chosen to ensure the inclusion of apps with significant presence and impact in Kenya'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 Kenya were included. Specifically, the study focused on apps like Bima[91], AfyaPap[92], MedAfrica,[93] and MyDawa,[94], all locally developed and recognised for their widespread use and impact on health in Kenya. A detailed case study of M-TIBA[95] is carried out to provide insights into the legal nuances emerging out of the health app. Additionally, a foreign-developed app, Ada[96], was considered due to its marketing efforts in the country and the availability of online information about its operation and use in Kenya.

The methodology is centred around an exploratory qualitative review of available online resources, including the websites of selected apps, scholarly articles, and reports detailing their functions, adoption patterns, user engagement, and their role in expanding health coverage and access. This review aimed to uncover the legal implications arising from the use of these apps, focusing particularly on terms of use, privacy policies, and data protection measures. The comparative analysis of these aspects across different apps provided insights into how health data is managed, shared, and protected, highlighting best practices and areas of concern.

In addition to the review of digital content, the study sought to understand the broader implications of app usage in Kenya, including ownership issues and intellectual property (IP) concerns. This involved analysing the funding mechanisms behind the apps, the partnerships that facilitated their development and deployment, and the regulatory environment governing digital health in Kenya.

2.2.2. Overview of the Digital Health Ecosystem

Stephanie and Sharma[97] present the digital health ecosystem as an intricate network of stakeholders like providers, payers, patients made feasible by digital platforms. Witte[98] sees the ecosystem as encompassing technologies, data and services – from electronic records to wearables to care delivery. Serbanati et al[99] consider the digital health ecosystem as the architecture enabling activities like care provision, service access and health monitoring. With this description, the health app ecosystem can then be described as one that refers to a network of digital health applications, platforms, and services designed to enhance healthcare delivery, patient engagement, and health outcomes. It involves

[91] https://bima-app.com/
[92] https://www.baobabcircle.com/about
[93] https://medafrica.org/
[94] https://africahealthitnews.com/kenya-mydawa-sceures-funding-to-become-an-all-in-one-health-platform-for-users/
[95] https://mtiba.com/
[96] https://ada.com/
[97] Stephanie, L and Sharma, R., 'Digital health ecosystems: An epochal review of practice-oriented research', *International Journal of Information Management* 53 (2020).
[98] Witte, A K., 'A Review on Digital Healthcare Ecosystem Structure: Identifying Elements and Characteristics', *PACIS 2020 Proceedings*, 228.
[99] Serbanati, L., Ricci, F., Mercurio, G et al., 'Steps towards a digital health ecosystem,' *Journal of Biomedical Informatics* 44:4 (2011) 621-636.

the integration of various technologies, including mobile apps, telehealth, electronic health records, and wearable devices, to provide accessible, efficient, and personalised healthcare solutions. This ecosystem connects patients, healthcare providers, and other stakeholders, facilitating the exchange of health information, remote monitoring, health financing, disease management, and health promotion activities, aiming to improve the quality of care and public health.

The health app ecosystem in Kenya interconnects various categories of apps to provide integrated healthcare solutions. For instance, teleconsultation apps like TIBU[100] facilitate patient-doctor video consultations, Sema Doc[101] enables chat-based diagnosis, while MedAfrica[102] and AfyaPap[103] share health information resources. On the patient data side, apps like M-TIBA[104] and eCHIS[105] maintain digital health records and exchange information with electronic medical record systems. Health apps also integrate with payment platforms like M-PESA[106] to enable services like insurance premium collection by Bima[107] and cashless claims settlement. App linkages also facilitate medicine delivery from e-pharmacies like MyDawa[108] arising from e-prescription on apps. Public health apps like KoviTrace[109] feed into health ministry dashboards to direct response. Such interconnections across mHealth, eHealth and fintech ecosystems pave way for remote patient monitoring, prompt interventions and streamlined regulatory processes.

Scholarship advanced by Neumark and Prince[110] as well as Townsend et al[111] reveal the health app ecosystem emerging in Kenya and provide some key insights into the digital health market. In terms of functionality, 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. In terms of the market, the ecosystem accommodates diverse business models – B2C, B2B2C - that each target unmet niche needs.[112] Distribution leverages the ubiquity of mobile devices rather than requiring access to specialist hardware.[113] Regarding infrastructure, interoperability is emerging both with national health insurance systems like NHIF as well as private platforms like M-PESA. Data integration through the Sasa Doctor app[114] spanning patient records, pharmacy systems and insurance claims also increasingly enable continuity of care.

Furthermore, Kenya's health app ecosystem demonstrates an interplay of locally developed apps and adoption of foreign solutions. On one hand, native startups are ideating mobile health innovations tailored to local needs. For example, Play Zuri Health's multi-functional Zuri platform enables appointments, teleconsultations, home services, and e-pharmacy delivery via app and SMS.[115] Its conceptualisation by Kenyan founders indicates growing digital health entrepreneurship targeting accessibility gaps. However, dependence on foreign capital persists. For instance, while Zuri Health's creators were local, MedAfrica's founders received European venture capital funding.[116] Other homegrown

[100] https://tibu.africa/

[101] Kariuki, D., 'Kenyans given 24 hour access to doctors through phone app', https://www.kenyans.co.ke/news/kenyans-given-24-hour-access-doctors-through-phone-app?page=20

[102] https://www.thehabarinetwork.com/kenyan-developed-medafrica-mobile-app-gaining-popularity-to-be-rolled-out-across-africa

[103] https://solve.mit.edu/challenges/health-security-pandemics/solutions/18964

[104] https://mtiba.com/

[105] https://chisuprogram.org/where-we-work/kenya

[106] https://www.vodafone.com/about-vodafone/what-we-do/consumer-products-and-services/m-pesa

[107] https://bima-app.com/

[108] https://mydawa.com/

[109] https://itweb.africa/content/mQwkoq6PgWk73r9A

[110] Neumark T and Prince R J., 'Digital Health in East Africa: Innovation, Experimentation and the Market', *Global Policy* volume 12, supp 6 (2021).

[111] Townsend BA, Sihlahla I, Naidoo M., et al., 'Mapping the regulatory landscape of AI in healthcare in Africa', *Front. Pharmacol.* 14:1214422 (2023).

[112] Ortigas-Wedekind, M., 'Digital Health Commercialisation: Considerations and Case Study', *Journal of Commercial Biotechnology*, 27:1 (2022), 20-7.

[113] Kumar P, Paton C, and Kirigia, D., 'I've got 99 problems but a phone ain't one: Electronic and mobile health in low- and middle-income countries', *Arch Dis Child* (2016)

[114] https://sasadoctor.co.ke/how-it-works

[115] https://www.zuri.health/

[116] https://medafrica.org/

startups like MyDawa,[117] Afya pap,[118] mUzima,[119] M-TIBA[120] also received sizeable external funding. This signifies ongoing reliance on external investors for scale-up, limiting organic business model sustainability.

Simultaneously, Kenya'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[121] and various others listed on the app stores then occurs locally. This facilitates transfer of effective health innovations across borders to benefit Kenyans, either for free or paid. While exogenous apps could crowd out local competition, they can also inspire domestic innovation. For example, under the project "There is No App for This"[122] a notable development is the MedAssist app, focusing on sickle cell disease. This app, accompanied by its chatbot named Mueni, is in the initial stages of development. Funding for this innovative endeavour is provided by the Wellcome Trust, exemplifying the kind of international support that is driving forward the health tech sector in Kenya. Such initiatives reflect a growing trend of blending local health needs with global resources and expertise. The health apps ecosystem in Kenya demonstrates a fascinating interplay between local innovation and global collaboration. This ecosystem reflects a pattern of blending local insights with global resources, creating a diverse and dynamic digital health landscape. Local developers, understanding cultural nuances and specific health challenges, innovate apps that resonate with Kenyan users. Meanwhile, foreign apps bring in technological advancements and broader health perspectives.

2.2.3. Categorisation of Health Apps

Platforms such as SimilarWeb[123] and AppFigures[124] provide a window into the vast array of health apps available in Kenya. They list 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.

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.[125] Erikson discusses the broader category of 'mobile phone apps', possibly encompassing a wide range of functionalities from patient engagement to data capture.[126] 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.[127] 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.[128] 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.

[117] https://africahealthitnews.com/kenya-mydawa-sceures-funding-to-become-an-all-in-one-health-platform-for-users/

[118] https://www.baobabcircle.com/about

[119] https://medium.com/usaid-2030/from-paper-health-records-to-muzima-the-mobile-health-app-that-helps-health-care-providers-do-1d3952940974

[120] https://www.crunchbase.com/organization/m-tiba/company_financials

[121] https://ada.com/

[122] https://warwick.ac.uk/fac/soc/law/research/centres/chrp/app/

[123] https://www.similarweb.com/top-apps/google/kenya/medical/

[124] https://appfigures.com/top-apps/google-play/kenya/medical

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

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

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

[128] 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.

Yasini and Marchand have proposed a methodological approach to classifying health apps.[129] 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. M-TIBA), public health management apps enabling outbreak surveillance (e.g. KoviTrace), pharmaceutical supply chain apps for medication inventory/delivery (e.g. MyDawa), and patient health records apps like e-CHIS 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.[130] The sheer volume of health apps, with approximately 350,000 in major app stores and around 90,000 new ones added in 2020,[131] presents an overwhelming challenge for 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 developing a method to classify health apps, especially within the Kenyan context, it is insightful to draw parallels with the methodology developed by Kay[132] 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 Kenya, it becomes evident that a nuanced classification system is required to cater to the diverse functionalities of health apps. In the Kenyan context, health apps can be seeing as serving various purposes ranging from telemedicine, as seen in Sema Doc[133], to health information platforms like MedAfrica[134], maternal health support through Jacaranda Health[135], and health financing with apps like MTIBA[136]. 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 Kenya, therefore, needs to be anchored in their

[129] Yasini M and Marchand G., 'Towards a use case-based classification of mobile health applications', *Studies in Health Technology and Informatics* (2015).
[130] Grand View Research, https://www.grandviewresearch.com/industry-analysis/mhealth-app-market#:~:text=The%20global%20mHealth%20apps%20market%20size%20was%20estimated%20at%20USD,USD%20105.9%20billion%20by%202030.
[131] IQVIA INSTITUTE. Digital Health Trends 2021 INNOVATION, EVIDENCE, REGULATION, AND ADOPTION. https://www.mobihealthnews.com/news/digital-health-apps-balloon-more-350000-available-market-according-iqvia-report (2021).
[132] Kay, R., 'Creating a Framework for Selecting and Evaluating Educational Apps', *Proceedings of INTED2018 Conference* 5-7th March 2018.
[133] https://expogr.com/detail_news.php?newsid=5338&pageid=2
[134] https://www.proquest.com/openview/721f94ce5d9a65932e734dbdf28da8d9/1?cbl=2042228&pq-origsite=gscholar
[135] https://jacarandahealth.org/
[136] https://mtiba.com/

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 Kenya 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 Kenyans, shapes a taxonomy for classifying health apps based on their functionalities and the health services they offer. The lived reality, including the widespread usage of smartphones and the cultural context, plays a crucial role in categorising these apps. For instance, Kenya's high internet usage, with 17.86 million internet users as of early 2023 and an internet penetration rate of 32.7 percent, reflects a digitally engaged population.[137] The presence of 10.55 million social media users, amounting to 19.3 percent of the population, and a striking number of 63.94 million cellular mobile connections, exceeding the total population, underscores the deep integration of digital technology in daily life.[138]

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 Kenyans. Arueyingho and Sanyaolu have noted the increasing prevalence of fitness apps, catering to the growing number of fitness enthusiasts in Africa.[139] This trend indicates the need for a specific category dedicated to health and 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 Kenyan 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: These apps enable virtual physician consultations and remote healthcare services. Examples include Sema Doc, My Dawa, TIBU Health, ConnectMed, and SASAdoctor.

b. Health Information Apps: These apps share knowledge resources on symptoms, diseases, and self-care practices. Notable examples are MedAfrica, AfyaPap, Totohealth, and My Daktari.

c. Patient Health Records Apps: This category includes apps that digitise, exchange, and monitor longitudinal patient treatment data. M-TIBA, Ministry of Health Kenya IMCI App and eCHIS are key players in this space.

d. Health & Wellness Apps: These apps focus on tracking fitness, biometric trends, and providing lifestyle change nudges. Zoezi, Jiactive, Flexpay, and My Fitness Pal are examples.

e. Personal Health Monitoring Apps: These apps capture individual health data for self-surveillance, such as period trackers, mDiabetes, My Health, and Afya Pap.

f. Diagnostic/Clinical Reference Apps: They include apps that use risk stratification algorithms or care guidelines to aid in health assessments, such as the Ministry of Health Kenya IMCI App (Integrated Management of Childhood Illness)[140]

g. Pharmaceutical Supply Chain Apps: These apps focus on delivering medication prescribed through virtual/remote consultation and inventory tracking. They serve as a marketplace for sale and purchase of medicines and medical equipment. My Dawa and Zuri Health are examples in this category.

h. Health Financing Apps: Apps that facilitate insurance policy purchases, premium payments, and claims processing fall into this category. Examples include M-TIBA, Bima, the NHIF app, Jamii, and M-Afya.

[137] DATAREPORTAL, DIGITAL 2023: KENYA, https://datareportal.com/reports/digital-2023-kenya

[138] DATAREPORTAL, DIGITAL 2023: KENYA, https://datareportal.com/reports/digital-2023-kenya

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

[140] https://nation.africa/kenya/healthy-nation/with-health-apps-you-now-have-a-personal-doctor-on-call-anytime-392146

i. Public Health Management Apps: These apps streamline surveillance, outbreak predictions, and data visualisation to enable responsive public health interventions. Examples include KoviTrace app[141] and Jitenge[142].

This proposed taxonomy for cataloguing health apps in Kenya serves as a valuable starting point, offering a systematic and structured approach to understanding and evaluating the country's health app ecosystem. By categorising apps into distinct groups such as Telemedicine, Health Information, Patient Health Records, and others, it provides a clear framework for users, healthcare providers, researchers and policymakers (collectively referred to as stakeholders) to navigate the diverse and complex landscape of digital health solutions. The taxonomy not only facilitates the selection of appropriate apps based on specific health needs and objectives but also lays the groundwork for comparative analysis. With this structured approach, stakeholders interested in learning about health apps, identifying an app based on its purpose or choosing a suitable app for personal use can effectively compare and contrast different apps within a category, assessing their functionalities, user-friendliness, effectiveness, and other critical parameters.

Furthermore, the taxonomy's utility extends beyond the Kenyan context. It provides a model that can be adapted and applied to other African countries, each with its unique digital health challenges and solutions. By using this taxonomy as a template, stakeholders in other African nations can categorise and analyse their own health app ecosystems, facilitating a broader understanding of digital health trends, needs, and opportunities across the continent and getting a mapping of the health apps under each category for cross country comparison. For example, MTIBA is prominent in Kenya as a health financing app, other such apps in different countries can be identified when listed under this category.

The classification system and comparative analysis for health apps, as proposed, also offer significant potential for a deeper understanding of the various risks associated with different categories of health apps in Kenya. By systematically categorising these apps, we can conduct a focused study on the specific terms of use for each category, offering insights into how these terms may vary across different types of health apps. A critical aspect of this analysis involves examining the terms and privacy policies of these apps. This examination can reveal how user data is collected, stored, and used, which is particularly pertinent given the sensitive nature of health information. By comparing terms and privacy policies across categories, we can identify commonalities and differences in data handling practices, providing a clearer picture of the data privacy landscape within the Kenyan health app ecosystem. This scoping study, however, will not address this aspect of comparative analysis across the categories but will instead focus on examining a single app as it functions within Kenya's digital health ecosystem looking at the regulatory framework, institutions and actors responding to the app. It will also review the terms of use and privacy policies of one locally developed app (M-TIBA) and a foreign app adopted in Kenya (Ada) to identify similarities and nuances.

Furthermore, issues around surveillance, user tracking, and data sharing are paramount. Different app categories might pose varying levels of risk in these areas. For instance, apps that track biometric data or personal health records might have different surveillance and data sharing implications compared to fitness or wellness apps. Future research will contribute to literature by analysing these aspects, so we can better understand how user data is potentially monitored and shared with third parties, whether for health monitoring, advertising, or other purposes. This comprehensive approach to analysing health apps goes beyond basic functionality to consider the broader implications of app usage, particularly in terms of user privacy and data security. Such an analysis is not only vital for informing users and healthcare providers about the potential risks associated with these apps but also for guiding policymakers and app developers in creating more secure and user-friendly digital health solutions that are legally protected.

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.

[141] https://itweb.africa/content/mQwkoq6PgWk73r9A

[142] https://www.mhealthkenya.org/covid-19

The dynamics of financing, funding flows, target segments, and intellectual property arrangements underpinning health apps align closely with key tenets of assemblage theory.[143] 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.[144] 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.[145]

For instance, Ogachi and Zoltan reveal that many Kenyan health apps rely considerably on foreign capital inflows, accumulating financial assemblages spanning investor locales like North America, and Europe.[146] Birhane explains that such dependence on external shareholders complicates local control,[147] potentially concentrating value outside health systems that most apps ostensibly aim to strengthen. This imbalance 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.[148] Consequently, investor demands, and proprietary constraints forestall user liberties customising code or data to suit local contextual needs. Such resulting exclusion, argue Freuler,[149] and Loo[150] 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 Kenya.

Some insights from the tensions between proprietary control, however, can be gleaned from Kenya's digital payments landscape, specifically the growth of M-PESA which provides lessons for the kind of ownership issues that health apps may also face. As the country's pioneering and widely used mobile money transfer service, M-PESA has been studied by Foster[151] as a prime example for analysis that parallels and reinforces the techno-social risks posited earlier around app ecosystems. The case of M-PESA exemplifies risks around external control over intellectual property rights that can also face health apps. M-PESA is widely lauded as an innovative digital platform that has achieved remarkable financial inclusion by connecting underserved populations in Kenya to vital financial services through mobile technology. As Ndung'u argues, by facilitating affordable money transfers, payments, and accessing credit for those excluded from formal banking, M-PESA has significantly advanced socioeconomic welfare.[152] However, beneath this empowerment narrative lies a complex ecosystem of proprietary technology, asymmetric partnerships, and intellectual property regimes that potentially concentrate value disproportionately into foreign hands.

Foster explains that while M-PESA operates extensive financial infrastructure powering Mobile Money transfers across Kenya, the originating code, patented technologies, algorithms and software systems underpinning its backend and functionality were predominantly built outside the country by foreign technologists.[153] Specifically, the

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

[144] 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.

[145] 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).

[146] Ogachi DO and Zoltan Z., 'Venture Capital and Silicon Savannah Valley in Kenya', In: Nasong'o WS, Amutabi MN abd Falola T (eds) *The Palgrave Handbook of Contemporary Kenya* (Palgrave Macmillan, Cham 2023).

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

[148] Ibid.

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

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

[151] 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.

[152] Ndung'u, N., 'The M-Pesa Technological Revolution for Financial Services in Kenya: A Platform for Financial Inclusion', In David Lee Kuo Chen and Robert Deng (eds) *Handbook of Blockchain, Digital Finance and Inclusion* (Academic Press, 2017).

[153] 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.

initial concept for M-PESA was developed by British telecommunications firm Vodafone in the early 2000s as an innovation project tailored for emerging markets based on research showing gaps in bank access. The company delegated engineers from its European headquarters to lead the coding, software architecture and encryption mechanisms enabling what became M-PESA's money transfer infrastructure accessible through basic mobile devices.[154]

Simultaneously, Vodafone's local joint venture Safaricom implemented the technical blueprint in Kenya by mobilising retail stores and mobile money agents into an integrated network. However, intellectual property rights over M-PESA's proprietary technology remained concentrated with Vodafone rather than researchers or businesses contributing expertise around Kenyan market conditions.[155] Consequently, Safaricom as licensee operator had to pay close to €170 million in royalty fees to Vodafone between 2010 and 2019 for permission to use systems substantially engineered abroad. Independent estimates project total royalty payments nearing €500 million in 2025 given M-PESA's exponential expansion.[156] This represents significant value leakage where Kenyan user revenue flows abroad rather than nourishing local digital infrastructures or rewarding contextual innovation by regional experts tailored for nuanced socio-cultural needs. This substantial value seepage through royalty payments exemplifies the commercialisation pressures exerted by proprietary ownership regimes able to disproportionately capture returns on local innovation. Safaricom's considerable royalty remittances approaching half a billion euros, though enabling vital infrastructure adoption, represent value redirection abroad that could otherwise fund public digital goods tailored for nuanced welfare needs.

Additionally, the rigidities from proprietary control over M-PESA's codebase worldwide risks marginalising open, collaborative digital innovation models that allow equitable value distribution to diverse contributors beyond principal shareholders. This is evidenced in comparisons with Tanzania's M-Pawa platform championed as exemplifying alternative approaches prioritising cooperative economic participation through codevelopment frameworks across public, private and civil society partners within East Africa.[157] In contrast, the concentration of core IP solely with Vodafone enables leveraging significant competitive advantages in mobile money markets across sub-Saharan Africa given control over technologies powering market-leading applications. M-Pesa replicates comparable offerings as it expands across geographies while restricting interconnectivity. Such dominance potentially crowds out opportunities for plural, inclusive innovation pathways that empower alternative local fintech enterprises across the continent advancing unique solutions for context-specific challenges.

These risks of disproportionate foreign capture of local creativity and exacerbated structural inequities observed in M-PESA's intellectual property regime carry valuable warnings as Kenya's health app ecosystem expands amidst digital transformations. While external investments enable scale, questions around data sovereignty, community agency, informed consent, privacy and equitable value distribution warrant attention before further app diffusion. As global capital permeates healthcare access, safeguarding public good duties calls for examining tensions between proprietary platform ownership models involving opaque third-party dependencies and end-user protections that respect participant dignity across digitally mediated treatment relationships.

The insights from examining M-PESA's proprietary technology ownership arrangements and value concentration risks carry important warnings for Kenya's health apps ecosystem which similarly relies on external investments and foreign systems integrations. The key problem is that this unfolding landscape currently lacks legislative safeguards or policy frameworks governing intellectual property regimes, open collaboration models and equitable value distribution across health app production networks. Several concerns also arise from the study of M-Pesa which offers a cautionary example regarding the risks around health apps:

Firstly, many promising health apps rely extensively on proprietary software, algorithms and technical integrations controlled by external multinational technology providers and venture capital investors seeking returns on financing support. This risks entrenching neo-colonial imbalances where platform IP concentrated abroad enables disproportionate value and data extraction outside local health systems, even when apps enhance access and inclusion. Secondly, dependence on foreign proprietary systems risks marginalising alternative open technology development pathways prioritising co-creation across diverse local experts who can enhance contextual effectiveness. However, rigid IP protections favouring primary shareholders with competitive consolidation aims can undermine such collaborative

[154] Ibid.

[155] Foster C., 'Global Transfers: M-Pesa, Intellectual Property Rights and Digital Innovation', Proceedings of the 1st Virtual Conference on Implications of Information and Digital Technologies for Development (2021).

[156] Ibid.

[157] Gama M., 'Killer Trade: Vodacom', *finweek*, no. 17 (2021).

innovation suited for local needs. Thirdly, in the absence of clear IP policy governing health apps, rigid proprietary regimes may gain dominance, concentrating power in external hands through competitive advantages. This crowds out cooperative platforms attempting contextual innovation through participatory design and inclusive ownership.

2.2.5. Lessons Learnt

This analysis of the health apps landscape in Kenya including the categorisation, techno-legal factors and risks inherent in dependence on foreign systems reveals several crucial gaps in knowledge and practice for Kenya. Firstly, the review of classification systems for health apps in literature and commercial repositories showed that existing categorisation methodologies have not kept pace with the tremendous diversification in app capabilities reshaping healthcare access and also there is limited literature around health apps categorisation. The taxonomy suggested in this scoping study classified apps based on their functionalities spanning patient-doctor virtual consultations, knowledge resources, digitised treatment records, fitness tracking, medication delivery, and outbreak surveillance dashboards. However, this taxonomy requires frequent upgrading as developers rapidly integrate advanced analytics, sensors, augmented reality, genome sequencing and other exponential technologies that could alter delivery models. Updating classification systems to align with diversifying real-world solutions rather than base only on policy documents forms an imperative knowledge building task.

Secondly, the analysis of funding flows behind health apps surfaced the extensive reliance of promising local innovations on foreign capital and possibility of proprietary systems controlled externally. This revealed conceptual gaps between widespread positioning of apps as progressively transforming access for underserved communities versus risks of value and data extraction that disproportionately benefit foreign technology shareholders over health systems that apps ostensibly aim to strengthen. Marginalisation concerns manifest acutely in the absence of clear legislative frameworks governing equitable value distribution and intellectual property protections specifically attuned for the health apps domain spanning public and private infrastructure.

M-PESA offers a cautionary precedent where laudable aims to enhance financial inclusion through grassroots mobile money innovation relied extensively on proprietary elements like algorithms, codebases and patented transaction methodologies produced abroad. This allowed significant private value capture by multinational owners through royalties rather than equitable public value distribution nurturing homegrown solutions addressing contextual priorities. The tensions reveal how app ownership structures function as complex sociotechnical assemblages negotiating overlapping interests, priorities and accountabilities across diverse stakeholders participating in production networks spanning conception to delivery. Scholarship[158] has demonstrated that external control over core proprietary elements allows exertion of excessive influence destabilising assemblage trajectories away from welfare aims as profits get rechannelled along isolated nodes located distantly.

The parallels visible in proliferation of apps built on imported software stacks and foreign venture capital spotlight risks of potential value leakage from Kenya's health ecosystem if unaccompanied by appropriate structural safeguards. In the absence of policies tailored for the app environment that balance sustainability with access as fundamental public good, rigid regimes enabling external capture could gain dominance. Health apps carry heightened risks around clinical surveillance, data extraction and switching costs once companies build predictive profiles determining insurance eligibility, creditworthiness, and access qualifications. Couldry and Mejias have warned against unregulated "data colonialism" where marginalised populations structurally constrained from technology ownership provide captive data reservoirs to seed innovations later commercialised into global products from which subjects cannot exit or demand equitable participation.[159]

Lastly, the scoping study has picked out dearth of literature on Kenya around transparency in tracing how user contributions get valued within general app production networks relative to foreign expertise inputs that predominantly control proprietary elements like code, algorithms and interface layers mediating participation. Although terms of service specify rights transfers and licensing restrictions implying exchanged value, opaque sublicensing agreements between local integrators, overseas technology providers and external aggregators obfuscates benefit flows along the chain. The resulting accountability gaps allow obscuring potentially inequitable reward apportioning justified behind

[158] Couldry, N., & Mejias, U. A. *The Costs of Connection*: *How Data is Colonizing Human Life and Appropriating It for Capitalism* (Stanford University Press, 2019).
[159] Ibid.

innovation aims uplifting underserved groups rather than transparently examining whether financial gains truly align with societal value additions.

These lessons spotlight gaps requiring urgent attention before app infrastructures become embedded given the lack of legislative safeguards governing emergent issues relating to privacy violations, value leakages or locked-in data extraction exposed during the analysis. Specifically, concerns over disproportionate foreign capture, marginalisation of collaborative local innovation and tensions between public healthcare duties and private profit incentives require regulatory corrections early when transformation patterns remain fluid rather than post-facto remediation once dependencies and path dependencies deepen. Therefore, addressing highlighted gaps calls for methodologies analysing risks around foreign control and proprietary pressures across health app production networks spanning conception to delivery.

2.3. The Case of M-TIBA

2.3.1. Method of Analysis

There is a clear gap in the literature studying the impacts of commercialisation and external technologisation specifically on Kenya's health app environment. This section turns towards an empirical examination of M-TIBA to explore whether the issues identified from the study of M-Pesa can be spotted within this health app. Building on the identified research gap and need for an empirical examination of M-TIBA, this section adopts a qualitative legal analysis methodology reviewing the app's publicly accessible terms of service and privacy policy documents. This entails a dual lens encompassing both literal and purposive interpretation of the legal terms constituting the M-TIBA user contract which is available on its website. The contract between PharmAccess with Safaricom for the development of M-TIBA, which is not in the public domain, is excluded from this analysis.

A literal analysis focuses on the precise terminology, phrasing and definitions enumerated in the terms of service and privacy policy texts as codified.[160] With respect to M-TIBA's terms of service, literal interpretation scrutinises the specific data handling allowances, intellectual property assertions, confidentiality commitments and limitations to liabilities as explicitly outlined in these documents. However, a purely literal reading risks overlooking implied meanings or broader intentions behind the legal constructions.[161] Hence a supplementary purposive perspective aids in evaluating the context, objectives and motivations underlying codified clauses to identify gaps between stated aims around consent, privacy and competing priorities that are implied.

This combined methodology drawing literal extraction of binding clauses along with evaluating embedded purpose allows generating multi-layered insights on risks around informed consent, control and value distribution in health apps ecosystems. For instance, literal analysis can parse definitions of private data, terms for sharing with third parties and breach notification commitments. Purposive lens then interrogates transparency provisions around actual third-party identities, secondary usage allowances concordant with consent and accountability procedures for data breaches. It examines who platform architectures empower and whom they marginalise.

This approach builds on scholarship studying gaps in purpose limitation,[162] data minimisation[163] and consent requirements[164] operationalising in digital infrastructures beyond ceremonial compliance. It is attuned to identify instances of user profiling, pervasive tracking and targeted advertising that violate principles of equitable platform governance despite formally articulated protections enumerating rights and rhetorical empowerment visions. Specifically, the approach looks to uncover loopholes and transparency omissions in disclosed policies that open backdoors for harnessing user data into proprietary assets or insights monetizable through advertising, and secondary

[160] Mitchell C., *Interpretation of Contracts* (Taylor & Francis, 2018).

[161] Ibid.

[162] Hahn I., 'Purpose Limitation in the Time of Data Power: Is There a Way Forward?', 7 *Eur. Data Prot. L. Rev.* 31 (2021).

[163] Biega A J and Finck M., 'Reviving Purpose Limitation and Data Minimisation in Data – Driven Systems', *Technology and Regulation* (2021); Rowe F., 'Contact tracing apps and values dilemmas: A privacy paradox in a neo-liberal world', *International Journal of Information Management*, vol 55 (2020).

[164] Koch S., 'The OK Is Not Enough: A Large Scale Study of Consent Dialogs in Smartphone Applications', 32nd USENIX Security Symposium 9-11 August (2023).

sales.[165] There is literature on user data being profiled for credit scoring[166] and insurance eligibility filtering[167] as well but this will not be explored as part of M-TIBA's examination due to paucity of literature on Kenya around these themes. Such transparency gaps then enable data accumulation practices without informed consent that scholarship identifies as underpinning emergent 'data colonialism' mechanisms. Hence the combination of literal and purposive investigation of binding documents provides robust analytical purchase into tensions between espoused principles and clandestine architecture influences undermining equitable participation.

Additionally, a purposive interpretation lens helps uncover legal implications arising from M-TIBA's interconnectedness with other health platforms and apps assembling treatment relationships. As a pioneer health wallet interfacing enterprises like Safaricom, hospitals, clinics, diagnostics centers and pharmaceutical supply chains, M-TIBA exemplifies the porous data flows, diffuse consent architectures and proprietary technology interdependencies manifesting in digital health assemblages worldwide. Purposively analysing its terms of service allows recognising emergent risks from actors integrated through obscure contracting chains. Such purposive investigation of terms of service helps justify urgent attention to establishing regulatory sandboxes explicitly examining health app ecosystems and contract law relationships underpinning their assemblages before further diffusion.

2.3.2. Legal Analysis of M-TIBA's Contractual Terms and Privacy Policy

2.3.2.1. Terms of Service

M-TIBA is a pioneering mobile health wallet launched in Kenya in 2016 through a collaboration between Safaricom, PharmAccess Foundation, and CarePay. It aims to advance universal and affordable healthcare access by leveraging mobile money infrastructure. Within a few years, M-TIBA has emerged as a leading health financing platform catering to a wide subscriber base through its convenient functionality integrated into everyday mobile money workflows. M-TIBA allows individual users to save and earmark funds for their medical expenses, receive social support contributions from family and friends, and make payments to accredited healthcare providers. Its primary target user segment encompasses economically vulnerable populations such as informal sector workers, rural communities, women and children - demographics typically excluded from financial security and quality healthcare access.[168] It also facilitates governments, donors and insurers to disburse funds as medical subsidies and insurance coverage directed to registered beneficiaries.

Beyond individual subscribers, M-TIBA has enrolled over 10,000 healthcare providers into its network spanning pharmacies, clinics, diagnostics centres and hospitals across urban and rural regions. Partner facilities can redeem payments instantly from serviced customers into their commercial bank accounts. M-TIBA thus assembles payers ranging from households to donors and purchasers from small neighbourhood shops to established health corporations onto a unified mobile money powered medical financing ecosystem. By ridesharing on Safaricom's extensive mobile infrastructure and M-PESA platform, M-TIBA enhances market adoption for digital health solutions that would otherwise struggle with consumer education barriers. It interoperates with government agencies like Kenya's National Hospital Insurance Fund (NHIF) to facilitate renewal premiums and cashless insurance claims settlement channelled straight to accredited hospitals. The interconnections between telcos, banks, health facilities and patients within M-TIBA's architecture demonstrates early advancement of Kenya's envisioned integrated digital health infrastructure. However, its dependence on Safaricom's proprietary systems risks vendor lock-ins constraining patient agency and data portability.

An initial analysis of M-TIBA itself in terms of its development by Safaricom and other partners raises several key issues that warrant further investigation. The first major area of tension stems from M-TIBA's heavy reliance on Safaricom's proprietary infrastructure and systems for its backend operations. This dependence raises transparency

[165] Baecker J, Engert M, Pfaff M et al. 'Business Strategies for Data Monetization: Deriving Insights from Practice', 15th International Conference on Wirtschaftsinformatik, March 08-11 (2020); Kaplan B., 'How Should Health Data Be Used? Privacy, Secondary Use, and Big Data Sales', *Cambridge Quarterly of Healthcare Ethics*, 25:2(2016), 312-329.

[166] Barddal JP, Loezer L, Enembreck F et al., 'Lessons learned from data stream classification applied to credit scoring', *Expert Systems with Applications*, Vol 162 (2020).

[167] Martani A, Shaw D and Elger B S., 'Stay fit or get bit – ethical issues in sharing health data with insurers' apps' *Swiss Med Wkly*, Vol 149, No 2526 (2019).

[168] Huisman L, van Duijn S, Rogo K., et al., 'A digital mobile health platform increasing efficiency and transparency towards universal health coverage in low- and middle-income countries', *Digital Health* 8 (2022).

concerns regarding data privacy and consent, as Safaricom's commercial data practices[169] allow much broader sharing and utilisation of user data compared to M-TIBA's more restricted health-focused data policy. There seems to be a disjunction and accountability gap between M-TIBA's limited health data use claims and Safaricom's pervasive data surveillance infrastructure that enables selling[170] or sharing[171] aggregated customer insights. Secondly, while M-TIBA outwardly espouses progressive patient empowerment principles aligned with open collaboration models that distribute value across diverse contributors, its reliance on Safaricom's proprietary infrastructure controlled from outside Kenya risks disproportionately concentrating profits abroad similar to debates over M-PESA's external intellectual property ownership. This threatens to marginalize local innovation efforts to build homegrown digital health platforms suited for contextual needs.

Thirdly, M-TIBA's promised tight restrictions on sharing personal health data solely for direct health service provision purposes seems practically undercut by Safaricom's vague allowances for passing data to unspecified third parties and exploiting information for internal secondary purposes like targeted advertising incompatible with ethical care.[172] This hampers meaningful patient consent over diffuse data flows across partnerships. There seem inadequate vetting protocols assessing declared security policies versus mismatched incentives of interconnected platform owners which becomes pertinent as app-mediated health delivery expands amidst complex dependencies. Finally, despite expanding access, M-TIBA's dependence on Safaricom's proprietary backbone controlled externally risks value leakage where profits flow out of the local health ecosystem to enrich distant shareholders. This threatens to entrench neo-colonial imbalances in health innovation spaces intended to empower marginalised communities.

A deeper analysis by interpreting the terms of service of M-TIBA that are available online on its website[173] reveals several concerns around ownership and control imbalances, third party data sharing without accountability, funding flow opacity and user safeguard erosion. Each of these concerns are addressed next.

Firstly, the terms define the CarePay Group entities as encompassing CarePay Limited and unspecified “affiliates” without further specificity on precise corporate ownership structure or geographic headquarters.[174] This drafting opacity regarding locus of central control leaves open the possibility of predominant foreign capture despite M-TIBA being positioned as a homegrown Kenyan mobile health innovation. The expansive rights assertion over all intellectual property pertaining to the M-TIBA platform software, codebase and algorithms also signals proprietary constraints limiting participative open innovation suited for local needs. User liberties are significantly curtailed regarding abilities to request modifications, interoperability or integration with complementary patient-centered solutions for enhanced relevance.

Secondly, the terms grant CarePay blanket discretion to share user personal and health information with unspecified ‘service providers’, ‘business partners’ and ‘group companies’ without corresponding accountability checks on actual data handling practices concordant with policy safeguards.[175] This data access provision threatens to contravene principles around purpose limitation and informed consent, especially given the sensitivity of medical information.

Thirdly, the terms of service affirm extensive, far-reaching assertions of intellectual property rights over the M-TIBA platform software, codebase, and algorithms.[176] These IP rights are concentrated with the CarePay Group members, which includes CarePay Limited and its unspecified "affiliates", as well as their technology licensors. This concentration of expansive IP rights signals rigid control over the core technical elements constituting M-TIBA's

[169] https://www.safaricom.co.ke/data-privacy-statements

[170] Purnell, J., ‘Safaricom staff caught in police “trap” after data fraud’, TelcoTitans 31 January 2022, available: https://www.telcotitans.com/vodafonewatch/safaricom-staff-caught-in-police-trap-after-data-fraud/4387.article

[171] Mwangi, D., ‘KRA to monitor mobile money transactions in real time’, *pulse* 28 Aug 2023, available: https://www.pulselive.co.ke/business/domestic/kra-to-monitor-transactions-in-real-time-after-integration-with-safaricom-airtel-and/7t00xj6

[172] Purnell, J., ‘Safaricom staff caught in police “trap” after data fraud’, TelcoTitans 31 January 2022, available: https://www.telcotitans.com/vodafonewatch/safaricom-staff-caught-in-police-trap-after-data-fraud/4387.article

[173] https://mtiba.com/terms/

[174] M-TIBA Terms of Service, Clause A. Introduction, https://mtiba.com/terms/

[175] M-TIBA Terms of Service, Clause B. M-TIBA Platform, Services and Healthcare Programs, sub-clause 1.3, Clause D. Distribution of Healthcare Programs, sub clause 8.2, Clause F. General Terms for all M-TIBA Services, subclauses 18.2.4; 18.6, https://mtiba.com/terms/

[176] M-TIBA Terms of Service, Clause F. General Terms for all M-TIBA Services, subclauses 18.5, 19 https://mtiba.com/terms/

functionality and digital infrastructure. It severely constrains participative open technology innovation tailored for local contextual needs. For instance, user liberties are highly limited regarding abilities to legally request platform modifications, interoperability with complementary systems, or integration of locally developed solutions that could enhance relevance.[177] Essentially, the centralisation of M-TIBA's originative IP exclusively with the CarePay Group enables them to exercise proprietary control and extract disproportionate value. This proprietisation risks marginalising collaborative digital innovation suited for nuanced local requirements. It parallels the concerns arising from M-PESA's external IP ownership, where Safaricom paid significant royalties for rights to utilise a technology controlled abroad.

Without transparency provisions requiring equitable value distribution,[178] the CarePay Group can potentially capture an outsized share of returns generated from grassroots implementation efforts localising M-TIBA's adoption. This compounds the opacity over foreign capture, since the Group's geographic base remains unspecified and there is no data available online to confirm this. Further analysis also indicates stark contracting imbalances as the terms provide CarePay unilateral authority to terminate user accounts without recourse or add new user fees sans participatory oversight.[179] Additionally, the terms grant CarePay expansive legal indemnity for disputes arising from service disruptions or errors, severely eroding consumer accountability seeking remedies from vulnerabilities imposed by digital infrastructures mediating access to vital care.[180]

Beyond these structural and ownership issues, there are also concerning issues around user data profiling, deficient consent architectures, and surveillance risks that arise upon examining M-TIBA's terms of service. The terms grant expansive rights for CarePay Group entities to share personally identifiable user information and sensitive health data with opaque third parties like unspecified 'service providers', 'business partners' and 'group companies' without corresponding accountability checks.[181] This violates data minimisation principles as has been explained in the general literature by Biega and Finck threatening unauthorised profiling, given the vagueness over data sharing extents.[182]

The extensive third-party data access provisions[183] defy meaningful user consent over health information flows to unidentified external actors for undisclosed purposes. Users cannot reasonably judge, constrain or opt-out of diffuse data sharing with vague actors, jeopardising informed consent. The terms further fail to incorporate data portability rights allowing straightforward health information transfers to alternative platforms. This compounds lock-in effects once M-TIBA mediates access and pools medical records.[184] Without portability, transition burdens and switching costs could prevent changing platforms despite dissatisfactions.

2.3.2.2. Privacy Policy

The legal analysis reveals that M-TIBA's reliance on Safaricom's systems provides backdoor integration into telco databases optimised for subscriber profiling, ad targeting and surveillance.[185] This is because M-TIBA's data practices are aligned with Safaricom's privacy policy as its backend infrastructure is provided by Safaricom.[186] Safaricom's privacy policy statement[187] allows sharing personal data with unspecified 'subsidiaries, partners and agents'

[177] M-TIBA Terms of Service, Clause F. General Terms for all M-TIBA Services, subclause 19.2 https://mtiba.com/terms/

[178] M-TIBA Terms of Service, Clause D. Distribution of Healthcare Programs, subclause 8.2, https://mtiba.com/terms/

[179] M-TIBA Terms of Service, Clause F. General Terms for all M-TIBA Services, subclause 17.2 https://mtiba.com/terms/

[180] M-TIBA Terms of Service, Clause F. General Terms for all M-TIBA Services, subclause 18.5 https://mtiba.com/terms/

[181] M-TIBA Terms of Service, Clause F. General Terms for all M-TIBA Services, subclause 15.1 and 20.1. https://mtiba.com/terms/ - These subclauses permit broad allowances to share user personal data and health information with unspecified "service providers", "business partners" and vague "group companies" affiliates.

[182] Biega A J and Finck M., 'Reviving Purpose Limitation and Data Minimisation in Data – Driven Systems', *Technology and Regulation* (2021).

[183] M-TIBA Terms of Service, Clause F. General Terms for all M-TIBA Services, subclause 15.2 and 20.2, https://mtiba.com/terms/ - these subclauses contain terms which permit diffuse data flows to opaque third parties without accountability over secondary usage or consent provisions to opt-out/withdraw sharing.

[184] M-TIBA Terms of Service, Clause F. General Terms for all M-TIBA Services, subclause 17.3, https://mtiba.com/terms/ - this subclause is an account termination clause and fails to incorporate options for users to export or port medical data to alternative platforms, compounding transition barriers.

[185] M-TIBA Terms of Service, Clause A. Introduction, subclause 1.1, https://mtiba.com/terms/ - in this subclause we see that direct technical and operational reliance on Safaricom systems is designed around subscriber profiling rather than health data purpose containment.

[186] Government of Kenya, Digital Health Act No 15 of 2023 (Nairobi: National Council of Law Reporting).

[187] https://www.safaricom.co.ke/data-privacy-statements accessed 12 January 2024.

involved in delivering services, credit agencies, survey firms and emergency contacts. Hence, despite M-TIBA's standalone privacy terms,[188] dependence on commercial infrastructure designed for data extraction defies claims around health data purpose limitation or protection from unauthorised monitoring. To confirm whether M-TIBA's privacy policy contains gaps, its thorough review is conducted next.

The privacy policy codifies blanket intellectual property dominance over the software, algorithms and codebase constituting M-TIBA's platform to CarePay, its opaque corporate affiliates and software licensors.[189] This concentration of expansive IP control signals constraints impeding participative open technology innovation tailored for evolving local requirements by empowered user communities. Instead, clauses cement gatekeeping restrictions limiting customisations to externally controlled proprietary elements underlying M-TIBA's trajectory in shaping healthcare access. Clause 1.1 of M-TIBA's privacy policy affirms that its platform backend and operational infrastructure relies extensively on systems provided by telecommunications giant Safaricom. This is further evidenced in Clause 5.B which covers 'Payer Healthcare Programs' - essentially insurance plans and benefits packages - delivered over the M-TIBA platform in cooperation with partners like health ministries and hospitals. Here the policy clearly states M-TIBA acts merely as a 'data processor' fully dependent on the digital frameworks set up by Safaricom for user identity verification, connecting patients to accredited facilities, claims submissions by hospitals and payments settlement into provider accounts. Without Safaricom's proprietary infrastructure spanning mobile money workflows, hospital linkages and subscriber identification databases, M-TIBA would lack the backbone to assemble its envisioned healthcare access ecosystem across payers, providers and consumers.

This systemic reliance on Safaricom's commercial infrastructure optimised principally for continuously monetising data accumulated from customer call patterns, transactions logs and mobile internet surfing habits, in my view, severely compromises privacy assurances within intersecting medical platforms like M-TIBA. For instance, Safaricom's own privacy policy reserves expansive rights to share insights gleaned from sensitive personal data like location, financial flows and web browsing frequencies with vague third party 'agents' and 'partners' for advertising and internal analytics unable to be traced by end-users. This contradicts M-TIBA's selective sharing commitments once interconnected. Therefore, dependence on Safaricom's pervasive surveillance infrastructure designed for subscriber profiling risks overwhelming M-TIBA's isolated health data protection pledges, creating accountability gaps regarding information utilisation flows and irreconcilable tensions with equitable consent norms vital for platform stewardship balancing public welfare duties with sustainability.

A further legal issue that flags out is M-TIBA's integration with the National Hospital Insurance Fund's (NHIF) app for insurance claims processing. This prompts serious privacy concerns based on the earlier discussions around M-TIBA's terms of service and privacy policy. Specifically, M-TIBA's terms of service foster an accountability void over sensitive medical records sharing between interconnected private partners. This void is facilitated by M-TIBA's systemic reliance on Safaricom's commercial data infrastructure which is designed principally for continuous subscriber profiling, and this risks overwhelming consent protections once M-TIBA functionally interlinks with digital frameworks optimised for customer surveillance and marketing over ethical data custody. This infrastructural immersion into unauthorised monitoring ecosystems could permit unregulated user tracking of the NHIF app users by assembled vendors, eroding patient safeguards. Further, the pronounced concentration of proprietary control and intellectual property assertions exclusively to CarePay Group hinders tailored innovation suited for local public health priorities. It structurally empowers distant private owners over participative decision-making around optimising the NHIF app. In turn this risks misappropriating people's health data into opaque commercial systems without collective consent or oversight.

2.3.3. The Case of Ada: Comparative Analysis

The analysis of M-TIBA's terms of service revealed its technical architectures opaque external dependencies, infrastructural immersion into proprietary systems and value extraction absent accountability. The porous data flows enabled through Safaricom's digital infrastructure on which M-TIBA is embedded currently characterises the health apps ecosystem. Are similar tensions encoded within foreign health apps penetrating Kenyan markets? A potential answer to this question lies in exploring the Ada app developed by the German based Ada Health GmbH.[190]

[188] https://mtiba.com/privacy-policy/
[189] https://mtiba.com/privacy-policy/, clause 19.
[190] https://ada.com/about/

A doctrinal review of Ada’s terms of service[191] through literal and purposive analysis reveals considerable parallels with M-TIBA regarding outsized centralisation of proprietary controls, expansive third-party data sharing devoid of accountability and overreaching limitations to legal liability.[192] 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.[193] Further, section 12.3 of Ada’s terms contain a presumption of consent to updated terms if user does not explicitly object within 30 days of receipt of amendments. This obfuscates continuous consent withdrawal rights.

Under section 3.2. Ada retains 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 section 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.

Having studied M-TIBA and Ada, this section now turns to reveal similarities and differences between the two apps. Both M-TIBA and Ada reserve centralised intellectual property dominance over originative software code, algorithms and core participation infrastructure elements strictly within parent companies registered abroad. This severely hampers open technology innovation tailored for evolving local requirements by precluding user community engagements customising deployments suited for contextual needs. Seemingly, the apps effectively function as opaque black boxes rather than participative platforms.

The apps also share a reliance on undisclosed third-party technologies, which become embedded into overall functioning. M-TIBA depends on Safaricom's digital infrastructure designed around subscriber surveillance and customer data monetisation. Similarly, Ada grants itself interoperability with social media APIs to harness personal usage patterns. In both cases, diffuse data flows with external actors lacking transparency foist unexamined consumer privacy risks. Furthermore, a review of modifications clauses within the apps reveal consent complexities like auto-renewal of updated terms or altered platform features simply via presumed user acceptance absent explicit objections registered within short intervals. These coercive negative consent models seriously undermine exercise of continuous permission withdrawal rights envisioned under evolving data sovereignty policy frameworks worldwide. They entrench 'take-it-or-leave-it' participation architectures benefitting platform shareholders rather than meaningful safeguards.

However, a key difference arises from M-TIBA's deeper structural entanglement with foundational national databases like NHIF insurance rosters and mobile money workflows now governing access. In contrast, Ada operates as a largely standalone app without comparable digital infrastructure immersion. This divergence has critical policy implications given Kenya's constitutional commitments positioning healthcare as a non-derogable public good rather than private commodity. It necessitates heightened stewardship over platforms like M-TIBA straddling across sectors to check value expropriation.

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

[192] https://ada.com/terms-and-conditions/, sections 1.3, 6.1, 6.4, 6.6.

[193] https://ada.com/terms-and-conditions/, section 5.5.

2.3.4. Lessons Learned

M-TIBA's integration within Kenya's health and financial services via Safaricom's infrastructure exemplifies the complexities of digital health solutions in enhancing healthcare access while ensuring data privacy and security. The app's reliance on Safaricom's proprietary systems introduces a critical examination point for the transparency of data practices and the autonomy of user consent. The legal analysis reveals a disjunction between M-TIBA's health-focused data use claims and the broader data utilisation capabilities of Safaricom, indicating potential gaps in accountability and privacy safeguards. This scenario highlights the broader implications of commercial and technological externalities on local health ecosystems, raising questions about data colonialism and platform governance.

Moreover, the analysis of M-TIBA's contractual terms and privacy policy underscores issues of ownership, control imbalances, and third-party data sharing without sufficient accountability mechanisms. These findings suggest a significant erosion of user safeguards against the backdrop of proprietary control by CarePay and its affiliates, alongside a lack of transparency in data handling practices. The legal scrutiny further exposes the potential for user data profiling, pervasive tracking, and targeted advertising despite formal protections offered under Kemya’s Data Protection Act 2019.

Comparatively, the Ada app's legal and operational framework mirrors several concerns identified in M-TIBA, including centralisation of proprietary controls and opaque third-party data sharing mechanisms. Ada's terms of service and privacy policy illustrate a similar trajectory of data accumulation, profiling, and commercialisation, raising parallel concerns about data sovereignty and user consent. However, Ada's operational model, distinct from M-TIBA's integration with Kenya's healthcare and financial services, presents unique challenges in terms of policy implications and stewardship requirements.

The juxtaposition of M-TIBA and Ada within Kenya's digital health landscape reveals critical insights into the governance of health data, the intersection of technology and healthcare provision, and the implications for user rights and privacy. These findings have revealed the need for robust regulatory frameworks that address the nuanced challenges of digital health platforms, which is missing in Kenya. Such knowledge gap therefore requires further research inquiring into the establishment of regulatory sandboxes to explore these ecosystems comprehensively and develop informed policies that protect user privacy, ensure data security, and promote equitable access to healthcare services.

The legal analysis also highlights a fundamental shift of the doctrine of privity of contract, especially in the context of digital health apps like M-TIBA and Ada. Traditionally, the doctrine dictates that contracts cannot confer rights or impose obligations arising under it on any person except the parties to it. However, the complexity of digital ecosystems, particularly in health apps, challenges this traditional understanding due to the intricate web of relationships and dependencies that extend beyond the direct user-service provider interface. In the case of M-TIBA, while the contract ostensibly exists between the platform (and by extension, CarePay) and the end-user, the reality of operational dependencies on third-party platforms like Safaricom, and the integration with other services such as NHIF, introduces a multi-layered structure of relationships that are not adequately addressed by traditional contract law. This arrangement complicates the notion of consent, as the user's agreement to M-TIBA's terms of service indirectly implicates them in a broader network of agreements and data-sharing practices to which they have not explicitly consented. The integration with CarePay, subject to its own contractual agreements which impact M-TIBA (and thus the user), exemplifies this complexity and the limitations of the privity doctrine in safeguarding user interests and data privacy within interconnected digital health ecosystems.

This analysis undertaken further underscores a significant knowledge gap in the current legal framework regarding the protection of user rights and data privacy in the face of evolving technological landscapes. The traditional principles of contract law, centred on certainty and predictability,[194] are indeed tested by the findings from the legal analysis of M-TIBA and Ada. The reliance on proprietary systems and the opaque sharing of data with third parties without explicit user consent or accountability challenge these foundational principles. The legal framework struggles to accommodate the realities of digital health platforms, where user data traverses multiple entities, each with its own set of terms and conditions that may or may not align with the user's expectations or the initial terms agreed upon with the primary service provider.

[194] DiMatteo L D., *Principles of Contract Law and Theory* (Edward Elgar Publishing Press, 2023).

The lessons learned from this analysis suggest a pressing need to re-evaluate and potentially reformulate the doctrine of privity of contracts to better reflect the complexities of modern digital services. Such reforms would need to consider how to effectively incorporate third-party rights and obligations within contractual frameworks without undermining the essential qualities of certainty and predictability that underpin contract law. This might involve the development of new legal constructs or the adaptation of existing ones to ensure that users' rights and interests are adequately protected in a landscape characterised by intricate and often opaque networks of relationships and data flows.

2.4. Conclusion

This initial scoping exercise on digital health and health apps in Kenya has generated valuable empirical and conceptual foundations towards further research on technological architectures, data sovereignty and nuances within contract law based on the terms and privacy policy of the health apps. The study has revealed significant knowledge gaps around the ability of traditional contract law principles such as privity, certainty and predictability to accommodate the intricate technical dependencies and diffuse data dealings manifesting across interconnected apps lacking accountability. It highlights the urgent need to re-evaluate legal frameworks to reinforce user protections against proprietary overreach in increasingly opaque platform-driven healthcare access environments.

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