GSAR Journal of Applied Medical Sciences ISSN: 2584-2323 (Online)

GSAR Journal of Applied Medical Sciences
ISSN: 2584-2323 (Online)
Frequency: Monthly
Published By GSAR Publishers
Journal Homepage Link- https://gsarpublishers.com/gsarjams-home/

Patient Data Protection in Tanzania's Digital Health System

By

Mbiki Mkude Msumi

Head of Department (Public Law) and Lecturer, Faculty of Law, The Open University of Tanzania. A highly accomplished Lawyer & Legal Scholar. 10 plus experience in case assessment & analysis, strategy, negotiations, and public speaking.

Article History

Received: 11/10/2024
Accepted: 22/10/2024
Published: 25/10/2024

Vol – 1 Issue – 10

PP: -20-25

Abstract

The article examines the challenges and opportunities associated with patient data protection within Tanzania's rapidly evolving digital health system. As Tanzania continues to adopt digital health technologies, the protection of patient data has become a critical concern. The article seeks to identify gaps in the legal and regulatory framework, assess the effectiveness of current data protection practices example e-health apps such as M-MAMA, Pigia Daktari App, Mobile Afya App, AfyaPap offer, AfyaPro, Daktari Popote, and Jambo Mama Health App, and explore potential strategies to enhance data privacy and security in the healthcare sector, particularly in the digital health app regime. The primary problem addressed by the article is the insufficient protection of patient data in Tanzania's digital health landscape. With the increasing reliance on digital health solutions, there is a growing risk of data breaches, unauthorized access, and misuse of sensitive patient information. The article highlights the need for robust data protection measures to ensure patient data's confidentiality, integrity, and availability.

Keywords: *Digital Health Apps, Patient Data Protection, Mobile Health (mHealth), Data Privacy*

1. Introduction

The World Health Organization approved integrated care in 2015 as a comprehensive solution to the growing complexity of today's healthcare needs. Integrated care guarantees that patients receive coordinated and continuous care at all system levels by dismantling silos and encouraging collaboration amongst diverse healthcare professionals. This model reduces fragmentation, avoids duplication of services, and promotes efficiency, which not only improves the quality of care but also improves patient outcomes. With integrated care providing a more patient-centered and sustainable healthcare framework, it is imperative to manage these changing challenges as people live longer and have more complex healthcare needs.[1]

The use of digital technology to improve accessibility, management, and healthcare delivery is referred to as a digital health system. It includes a broad range of instruments, platforms, and technologies, including wearables, mobile health apps, telemedicine, electronic health records (EHRs), and health information systems.[2] Patients and healthcare practitioners may communicate more effectively because to these systems' efficient and safe methods of gathering, storing, and analyzing patient data. Digital health systems use technology like artificial intelligence (AI), machine learning, and big data analytics to provide remote monitoring, individualized treatment, and data-driven decision-making.[3]

A digital health system can save costs and improve patient outcomes while also increasing the efficiency of healthcare delivery. Healthcare providers can minimize medical errors and streamline workflows, while patients can access care more conveniently, especially with the help of telehealth services. Furthermore, by facilitating the easy sharing of patient data, digital health systems promote cooperation among multidisciplinary healthcare teams. This change is especially helpful in underserved and rural areas, where

[1] *Jimenez J, del Rio A, Berman AN, Grande M. Personalizing Digital Health: Adapting Health Technology Systems to Meet the Needs of Different Older Populations. Healthcare. 2023*

[2] *Bhumi Shah, John Lee Y. Allen, Hassan Chaudhury, James O'Shaughnessy, Carina S.B. Tyrrell, The role of digital health in the future of integrated care, Clinics in Integrated Care, Volume 15, 2022,*

[3] *Ibid*

*Corresponding Author: **Mbiki Mkude Msumi.**

access to high-quality healthcare can be scarce. It closes gaps in healthcare delivery and enhances public health in general.

Health applications are software programs that can be used as accessories or combined with mobile devices like smartphones and tablets. They enable digital diagnostic and treatment standards, empowering patients and healthcare professionals. These applications help patients understand and manage their health conditions, providing guidance and assistance, and improving healthcare practitioners' efficiency and intelligence.

The use of digital health apps is on the rise globally. The rise of digital health apps in Tanzania holds great promise for improving healthcare delivery, enhancing access to services, and empowering individuals with the knowledge and tools to manage their health more effectively.[4] As technology continues to advance and more people gain access to digital devices, the impact of these health apps is likely to grow even further. These Apps mainly focus on managing health conditions such as chronic diseases. They have improved accessibility by eliminating the social stigma of visiting doctors in person. In addition, consumer health apps help people keep track of their health by monitoring daily steps and accessing exercise and nutrition programs. Most apps can collect, store, and share patient data. Therefore, protecting patient data is a crucial ethical consideration requiring regulatory compliance.

Only 110 health-related apps have been downloaded more than 10 million times, which accounts for almost half of all downloads.[5] Apps that fail to follow guidelines, do not function as intended, are out-of-date, or are economically unviable due to the ongoing costs of continually updating to new operating systems are typically removed from the app stores.[6] Many low-quality and unsafe health apps and potentially harmful content exist.[7]

Daktari Popote and **AfyaPap offer** remote consultations and appointment booking services, reducing waiting times and streamlining patient management. **AfyaPro** assists in managing chronic diseases like diabetes and hypertension by providing tools for monitoring conditions, accessing medical records, and receiving medication reminders. These apps help people in remote areas access healthcare services.

Data security and privacy concerns have grown with the increasing use of digital health apps. Regulations like GDPR in Europe have set a precedent, and similar regulations are being discussed or implemented in various countries. Almost 88% of health apps collect and potentially share user data, making data management and protection crucial ethical considerations and requiring regulatory compliance.

The regulation of digital health apps and the protection of patient data are fundamental to ensuring users' safety, privacy, and trust, promoting innovation, preventing misuse, enhancing interoperability, and supporting public health initiatives. The regulation of digital health apps and the protection of patient data are fundamental to ensuring users' safety, privacy, and trust. As these apps become increasingly integrated into healthcare systems, stringent regulations are essential to prevent potential risks such as data breaches, unauthorized access, and misuse of sensitive information. Robust regulatory frameworks provide guidelines and standards that developers must adhere to, ensuring that digital health solutions are reliable and secure. This fosters a sense of trust among users, who can be confident that their personal health information is handled with the utmost care and confidentiality.

Moreover, well-implemented regulations promote innovation in the digital health sector. By setting clear standards and expectations, regulatory bodies can encourage developers to create apps that are not only innovative but also compliant with privacy and security requirements. This balance between regulation and innovation helps prevent stifling creative solutions while ensuring that new technologies contribute positively to the healthcare system. Additionally, regulations can drive interoperability, making it easier for different health apps and systems to work together seamlessly, thus enhancing healthcare delivery's overall efficiency and effectiveness.

In a broader context, regulating digital health apps and protecting patient data support public health initiatives. Accurate and secure data collection and sharing are crucial for monitoring and responding to public health threats. Regulations ensure that data used for public health purposes is collected ethically and utilised appropriately, helping to prevent misuse and ensuring that public health agencies can rely on high-quality data. This regulatory oversight is vital for maintaining public trust in digital health solutions and leveraging these technologies to improve population health outcomes.

2. Current State of Digital Health in Tanzania

The landscape of digital health apps in the country is rapidly evolving, driven by technological advancements, the increasing prevalence of chronic diseases, and the demand for more accessible and personalized healthcare solutions. The country initiated the use of digital technology in healthcare

[4] *World Health Organization. WHO guideline: recommendation on digital interventions for health system strengthening: web supplement 2: summary offindings and GRADE tables. World Health Organization; 2019. Accessed on September 10, 2024 at https://www.who.int/reproductivehealth/publications/digital-interventions-health-system-strengthening/en/*

[5] *Emily M., "How digital health apps are empowering patients, improving outcomes, and increasing accessibility", Deloitte Centre for Health Solutions, 2021*

[6] *Emily M., "How digital health apps are empowering patients, improving outcomes, and increasing accessibility", Deloitte Centre for Health Solutions, 2021*

[7] *Larsen ME, Nicholas J, Christensen H. A Systematic Assessment of Smartphone Tools for Suicide Prevention. One 2016*

*Corresponding Author: **Mbiki Mkude Msumi.**

during the 1990s.[8] They began by digitizing the country's health management system. This allowed for data collected from local health facilities to be used for planning at the district level.[9] Hospitals performing research and clinical trials, especially on HIV, then began to go digital. As such, the spread of digital health technology in Tanzania seems similar to its dissemination in high-income countries.[10] The Government of Tanzania is committed to improving the application of digital health technologies to facilitate the attainment of its overall objective of delivering high-quality health services to all citizens. This is evidenced by implementing the National eHealth Strategy 2013–2018 to accelerate the health system transformation by enabling timely information access and supporting healthcare administrative, financial, and clinical operations to enhance decision-making.[11]

The number of digital health apps in Tanzania has grown tremendously. These apps have become essential tools for health practitioners, both healthcare providers and patients. The applications provide an opportunity to reduce the burden on health systems countrywide. The growth of these technologies has brought several developments in the health industry; however, due to these developments, e-Health and mobile health have raised privacy concerns for both healthcare providers and patients in Tanzania and the rest of the world.

The app M-MAMA is an emergency transport system in Tanzania, and it helps pregnant women get transport and receive emergency care. M-MAMA serves as a conduit between pregnant women and the healthcare systems, principally those at lower risk, by linking the gap in access to quality healthcare. Data security, privacy, and trust remain critical concerns in data protection regimes and digital healthcare platforms. The president further ordered the Ministry of Health to ensure the M-MAMA app becomes sustainable, simple, and meets the intended objectives. Up to now, the M-MAMA app has managed to save the lives of expected mothers and newborns who needed emergency services by connecting them with nearby ambulances and rushing them to the health facilities. The program will now be implemented in at least 20 regions nationwide.

In 2021, Agha Khan Health Services in Tanzania launched the **Pigia Daktari App.** The app complements the government's efforts to use technology to enhance access to quality healthcare delivery services across Tanzania. This telemedicine mobile app helps Tanzanians access medical specialists' care safely and quickly in urban and remote areas. This app offers special consultations for patients who cannot travel a distance to seek medical care and those who do not wish to be seen by people within their community and prevail over their privacy issues. Patients here have the right to choose doctors and seek help immediately.

The statistics show a ratio of 1 doctor to 20,000 patients in Tanzania, which is quite a considerable number. The **Mobile Afya App** is an offline mobile application technology that provides primary health information in native languages such as Swahili. This application has advantages as it works on offline phones and smartphones. The developers of this app include medical professionals, doctors, engineers, and technical innovators.

Jambo Mama Health App. It is an innovative solution that helps save the lives of expectant mothers who live far from health facilities and can deal with gynaecological obstetric emergencies.[12] It is an interactive mobile application that connects pregnant women living with the mother and child healthcare services. It organizes pregnancy surveillance, alerts when it is time for an antenatal check-up, and asks questions and updates of vital data that enable the detection and prevention of vital risks for mother and child, thus avoiding untimely, tiresome, expensive, and dangerous trips to the health facility.[13]

The primary beneficiaries are Pregnant women in rural areas of developing countries who live far from adequate healthcare services. If their pregnancy is monitored correctly, they'll be safer, more confident, empowered with relevant information and advice, and able to better manage their health needs during pregnancy. Their unborn child, as a significant number of stillbirths and congenital disabilities, will be avoided. At the same time, the newborn will have a live mother to care for him—the baby's siblings, who can be nurtured by their mother, who survived childbirth.[14]The development of Health Information Technology in general and electronic health records in particular is being pushed worldwide.[15] Globally, information and communication technologies, known as eHealth, play an increasingly integrated role in providing and managing health care and medical services.[16]

---

[8] *Geoff, W.," The Tanzanian digital health agenda", The Lancet Digital Health: Vol 2: 2020.*

[9] *Ibid*

[10] *For more on the Tanzania National e-Health Strategy (2013–18) see http://www. tzdpg.or.tz/fileadmin/ documents/dpg_internal/dpg_ working_groups_clusters/ cluster_2/health/Key_Sector_ Documents/Tanzania_Key_ Health_Documents/Tz_eHealth_ Strategy_Final.pd (accessed 16.3.2023)*

[11] *Tanzania-Ministry of Health, Community Development, Gender, Elderly and Children, Digital Health Strategy July 2019 - June 2024 http://api-hidl.afya.go.tz/uploads/library-documents/1573688147-xrkVuNtD.pdf (accessed 16.3.2023)*

[12] *https://www.healthynewbornnetwork.org/blog/jambomama-new-health-mobile-app-tanzanian-women/ (accessed 18.3.2023)*

[13] *Ibid*

[14] *Ibid*

[15] *Verhenneman, G and Dumortier, J., 'Legal Regulation of Health Records: A Comparative Analysis of Europe and the US' in George, C et al., eHealth: Legal, Ethical and Governance Challenges, Springer, Heidelberg/New York/Dordrecht/London, 2013, pp.25-56, at p.25.*

[16] *George, C et al., eHealth: Legal, Ethical and Governance Challenges, Springer, Heidelberg/New York/Dordrecht/London, 2013, (accessed 19.03.2024)*

*Corresponding Author: **Mbiki Mkude Msumi.**

3. The law on digital health apps in Tanzania

In Tanzania, while there is no specific law governing digital health apps, several broader legislative frameworks address privacy and confidentiality in the handling of personal data. The Cybercrimes Act, 2015 and the Electronic Transactions Act, 2015 include provisions on data protection, focusing on preventing unauthorized access, modification, and misuse of data, which can be applied to digital health information. Additionally, **The United Republic of Tanzania Constitution 1977 as ammended** indirectly provides for the right to privacy under Article 16, which protects personal information from arbitrary interference. However, none of these laws are tailored to the specific sensitivities and nuances involved in processing health data through digital platforms, leaving gaps in protection. These laws emphasize a general approach to data protection without addressing healthcare-specific challenges such as patient consent, data ownership, or how health data should be shared or stored.

The convergence of these laws lies in their intent to safeguard personal data and ensure privacy across digital interactions, including health-related information. However, they diverge in their scope and application. While the Constitution provides a broad right to privacy, it lacks detailed guidelines on the specifics of data protection in the context of digital health. **The Cybercrimes Act 2015** and **Electronic Transactions Act 2014** focus more on combating cybercrime and regulating online transactions, respectively, rather than addressing health data confidentiality directly. For instance, the **Tanzania Personal Data Protection Act 2022** provides a comprehensive framework for data protection in Tanzania. It covers informed consent, data subject rights, and cross-border data transfers. Digital health apps must ensure compliance with the principles of lawful data processing, data minimization, and security. The Act regulates the transfer of personal data across borders, which is particularly relevant for digital health apps that store data on international servers or involve international collaboration. This lack of a unified, health-specific data protection framework creates inconsistencies and uncertainty in how patient data is handled, especially when exchanged through digital health apps. As a result, these general laws may not provide adequate protection for sensitive health information, raising concerns about privacy in the growing digital health sector.

The Constitution of the United Republic of Tanzania of 1977 as ammended

Article 16 (1) states, *"Every person is entitled to respect and protection of his person, the privacy of his person, his family, and his matrimonial life, and respect and protection of his residence and private communications."* According to Article 16, an individual has a right to privacy in his person, family, and marital life. Tanzania has a data privacy legislation, the **Personal Data Protection Act, 2022**, that affects the constitutional right to privacy section 9 of the Act prohibits the processing and further processing of previously collected personal data, unless the data subject authorizes the processing or data processing is provided by law or data is processed concerning the purpose of collection. Similarly, the Act prohibits in section 10(1) disclosure of already collected data to anyone except the data subject. There are only a few exceptions that permit disclosure, such as where a data subject has expressly or implicitly consented or under the compulsion of the law or if it is disclosed in relation to the purpose of collection.

The Medical, Dental, and Allied Health Professionals Act, 2008

The Act established the Allied Health Professions Council, the Medical and Dental Council, the Nursing and Midwifery Council, the Pharmacy Council, and the Psychology Council to provide for related purposes. The code, among other things, provides for the principle of confidentiality concerning medical, dental, and allied health. On the other hand, the **Public Health Act**[17] governs the overall health sector in Tanzania, including using health-related technologies. This Act sets out the responsibilities of the Ministry of Health in regulating public health services, which may extend to digital health applications. The Tanzanian Government enacted the HIV and AIDS (Prevention and Control) Act in 2008. The Act is very comprehensive, covering all aspects of HIV and AIDS prevention, treatment, and community response. Section 16 of the Act provides about the confidentiality principle regarding the HIV results, and section 17 provides about the same principle but concerning medical confidentiality in dealing with the person living with HIV. So, this Act protects data privacy in E-Health but only with the people living with HIV/AIDS.

The Cybercrimes Act 2015

This Act addresses issues related to cybersecurity, including personal data protection. Digital health apps must implement measures to safeguard against unauthorized access to sensitive health information. As a penal law, the application of the Cybercrimes Act is not restricted if the offences were committed within the United Republic of Tanzania, including on vessels or aircraft registered in Tanzania. The Act would also apply to Tanzanian nationals residing abroad if the Act committed is an offence both in Tanzania and under the laws in the host country. Further, the Act applies to any person, regardless of nationality, if the abuse or violation (i) is committed using a computer system, device or data located within Tanzania or (ii) directed against a computer system, device, data or person in the Republic. It is an offence to access or cause a computer system to be accessed without permission. Anyone who commits this offence will be imprisoned for a year or a fine of not less than three million Tanzanian Shillings or both fine and imprisonment.

It is an offence to remain in a computer system intentionally and unlawfully or to continue to use it after the expiration of the time that one was allowed. Doing so is punishable by imprisonment of not less than one year or a fine of not less than one million Tanzanian Shillings or both. Similarly, intercepting personal communications and interfering with

[17] *Enacted in 2009.*

*Corresponding Author: **Mbiki Mkude Msumi.**

data by damaging, deleting, altering, obstructing or interrupting it is an offence. The penalty is a fine of not less than ten million Tanzanian Shillings, or three times the value of undue advantage received by the offender, whichever is more fantastic, or imprisonment for a term of not less than three years. Further, the Cybercrimes Act prohibits operators and other service providers from monitoring activities or data being transmitted in their systems. However, they are also shielded from being held liable for illegal activity within their networks or systems through their actions.

Apart from the Constitution, some statutory laws have implications for privacy protection in the health sector. One of these laws is the Medical Practitioners and Dentists Act, Cap. 152 (R.E 2002). The Code of Ethics and Professional Conduct for Medical and Dental Practitioners in Tanzania 2005, established under the Medical Practitioners and Dentists Act, lays down two essential principles. The first is that the practitioner shall offer treatment and other health interventions to a client only after obtaining the client's informed consent. This is called the principle of self-determination. The second principle is based on the concept that records, interests, and affairs relating to the client's health are only confided to the practitioner.

Rule 4.0 provides about the principle of privacy, which is based on the concept that records, interests, and affairs relating to the client's health are confided to the practitioner only. Further, Rule 4.1 provides respect for a client's privacy while providing treatment and any other forms of interaction, and it shall avoid acts that are degrading, insulting, interfering with, or injuring the self-value of the client. The code protects privacy and data in the health sector through the two rules. The problem with the code is that when it was created, hospitals in Tanzania were not using the E-Health system or the digital health apps.

Information and Communication Technologies (ICT) Policy, 2016 outlines the government's approach to ICT development, including promoting e-health initiatives. The policy encourages digital technologies in healthcare while emphasizing the need for proper regulatory oversight.

Where these laws converge is in their overarching aim to protect personal data from misuse and unauthorized access, regardless of the platform or industry, including healthcare. However, they diverge significantly in their application to health data. The Constitution 1977 still offers broad protection but lacks detailed implementation mechanisms. The Cybercrimes Act 2015 focuses on punishing offenders in the digital space without providing a clear regulatory framework for data privacy in healthcare. Meanwhile, the Electronic Transactions Act 2015 centers on securing digital communications but does not address patient consent, confidentiality, or data sharing in healthcare settings. This divergence leads to gaps in the protection of patients' digital health information, as no law directly governs the privacy of data shared through health apps.

4. Digital health apps' data privacy and security challenges

The increasing use of e-health applications in Tanzania has raised significant concerns regarding data security. Many of these apps collect sensitive health information from users, which, if not properly secured, can be vulnerable to cyberattacks, unauthorized access, or data breaches. Given the limited digital infrastructure and awareness around cybersecurity, protecting patient data from malicious actors becomes a challenge. Weak encryption standards and insufficient protective measures within these apps make it difficult to ensure the confidentiality and integrity of personal health data. Unlike traditional healthcare providers, many digital health apps are not subject to strict regulatory standards. This lack of oversight can lead to inconsistent privacy practices and security protocols. Digital health apps often collect a wide range of personal data, including sensitive health information, location data, and usage patterns. This data can provide valuable insights and pose risks if not adequately protected.

In addition to security issues, privacy concerns are also prevalent. e-Health apps in Tanzania often require users to input detailed personal information, including medical history and biometric data. However, many users are not fully informed about how this data is stored, shared, or used by third parties. There is also the risk of data misuse, as regulations around data protection are still in development. This lack of transparency can erode user trust and discourage the widespread adoption of digital health services. In data breaches or misuse cases, it can be difficult to determine who is responsible, particularly when data passes through multiple parties. Some health apps lack forceful encoding for data storage and transmission, making sensitive information vulnerable to interception and unauthorized access.

The health sector is particularly vulnerable to cyberattacks due to the highly sensitive nature of the data it handles. Medical records contain detailed personal information, including names, addresses, Social Security numbers, and health histories, which makes them valuable targets for cybercriminals. Breaches in this sector can lead to severe consequences, such as identity theft, fraud, and unauthorized access to medical histories, which can be used for various malicious purposes.

Furthermore, the issue of informed consent is a critical concern in the use of e-health apps. Many users may not fully understand the implications of providing their health information to these platforms due to complex terms and conditions, which are often written in technical language. In some cases, patients may not be adequately informed about how their data will be utilized, shared with healthcare providers, or processed for research purposes. This lack of clear communication can lead to violations of patient autonomy, as individuals are unable to make fully informed decisions about the use of their personal health data

.

*Corresponding Author: **Mbiki Mkude Msumi.**

5. Conclusion and recommendations

The fields of virtual consultations, remote monitoring, mobile health apps, digital therapeutics, and artificial intelligence have demonstrated success in leveraging digital health to shape the future of integrated care. Connecting data silos across the continuum of care is a significant challenge to achieving integrated care, and this raises concerns about data security and privacy. The healthcare system's culture and digital skill set are evolving.

Tanzania's digital health app regulatory environment is indeed evolving, reflecting the country's broader efforts to modernize its healthcare system and ensure patient safety in the digital age. Developers and healthcare providers must stay informed about the latest laws, regulations, and guidelines to ensure their products and services comply with the legal requirements. As digital health apps often handle sensitive patient data, understanding and complying with data protection laws, such as the Tanzania Personal Data Protection Act 2022 or relevant provisions within broader laws, is crucial.

Regulating digital health apps is crucial for ensuring patient safety, data privacy, and the efficacy of health interventions. However, the rapid growth of digital health technologies has outpaced existing regulatory frameworks in many regions. Data privacy laws must be enhanced to include specific provisions for digital health apps, ensuring that sensitive health data is securely stored, transmitted, and used. The government must develop standardized definitions for a digital health app, distinguishing between medical devices, wellness apps, and health information platforms. There is a need to establish a risk-based classification system that differentiates between apps based on their potential impact on patient health. It is important to establish mechanisms for patients and healthcare providers to report issues with digital health apps, as it can inform regulatory actions and updates. There is a need to promote policies that ensure digital health apps are accessible to all, including provisions for affordability, language accessibility, and usability for individuals with disabilities.

Staying informed and proactive in understanding the regulatory landscape will help developers and healthcare providers navigate compliance and contribute to the safe and effective use of digital health technologies in Tanzania. These reforms and policy recommendations aim to create a regulatory environment that balances innovation with patient safety, data security, and ethical considerations, ultimately leading to better health outcomes and a more robust digital health system.

REFERENCES

1. Makame, M. & Mujinja, P. G. M. (2021). "The Legal Framework for Data Protection in Tanzania: Implications for Healthcare." Journal of Digital Health and Law, 12(2), 145-163.
2. Nungu, A. M., & Moshi, A. G. (2019). "Data Protection Challenges in eHealth Systems in Developing Countries: The Case of Tanzania." African Journal of Health Information Systems, 7(1), 34-47.
3. Muriithi, P., & Lungo, J. (2018). "Ethical Considerations in Managing Patient Data in Tanzania's Health Management Information System." BMC Medical Ethics, 19(1), 56-65.
4. Kinyili, K. (2022). "Tanzania's Road to Digital Health: Infrastructure, Legislation, and Data Privacy Concerns." Global Health Informatics Journal, 11(3), 89-103.
5. Ndunguru, L., & Tarimo, D. (2020). "Health Data Privacy and Security Issues in Tanzania: The Role of the Data Protection Act." Journal of African Health Law and Policy, 15(2), 124-137.
6. Lema, R. & Mwang'onda, E. (2017). "Implementing Digital Health Systems in Tanzania: A Review of Legal and Privacy Concerns." International Journal of Digital Healthcare, 10(4), 102-119.
7. World Health Organization (WHO). (2020). "Data Governance and Digital Health in Low-Income Countries: The Case of Tanzania." WHO Digital Health Reports, 30-52.
8. Shadrack, P. & Maro, G. (2021). "Tanzania's Health Information System: Digital Evolution and Patient Privacy Protections." East African Medical Journal, 98(7), 311-329.
9. Munisi, J. & Kyando, J. (2023). "Patient Confidentiality and Data Security in Tanzania's Digital Health Sector: Current Status and Recommendations." Journal of Healthcare Data Protection, 9(1), 54-73.
10. Paul Cerrato, (2013). "Protecting Patient Information: A Decision-Maker's Guide to Privacy, Security, and Health IT" CRC Press.
11. European Commission (2016). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 of the European Parliament and of the Council. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
12. United Nations Conference on Trade and Development (UNCTAD) (2021). Data Protection Regulations and International Data Flows: Implications for Trade and Development. UNCTAD Study. Available at: https://unctad.org/webflyer/data-protection-regulations-and-international-data-flows-implications-trade-and-development
13. Institute of Medicine (US) Committee on Regional Health Data Networks, "Health Data in the Information Age: Use, Disclosure, and Privacy", National Academies Press: 1994.

*Corresponding Author: **Mbiki Mkude Msumi.**