Journal of Posthumanism

2025
Volume: 5, No: 12, pp. 140–156
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i12.3738

Posthuman Dataflows: Passive Data Migration and Algorithmic Sovereignty in East Africa

Elijah B. Ndemo[1], Dr. Ben Mkalama[2]

Abstract

This study conceptualizes Passive Data Migration (PDM) as a posthuman process through which health data, infrastructures, and algorithms acquire agency in shaping governance across East Africa. As predictive analytics, artificial intelligence, and global health platforms collect and transmit sensitive information, data move beyond national and human control, enacting new relations of power between human and nonhuman actors. Drawing on mixed-methods research in six East African nations, the study reveals how inadequate local infrastructure, donor dependency, and external demand create a digital ecology where databases, cloud systems, and algorithms function as autonomous participants in decision-making. These findings are interpreted through the lenses of data colonialism and data justice, showing how posthuman entanglements displace traditional ideas of sovereignty and accountability. The article argues for re-imagining data governance as a distributed ethical field in which both human and technological entities share responsibility. It concludes by proposing a regional framework for equitable data protection that recognizes algorithmic and infrastructural agency as integral to East Africa's digital futures.

Keywords: *Passive Data Migration; Posthumanism; Data Sovereignty; Algorithmic Agency; East Africa; Data Colonialism.*

Introduction

Passive Data migration (PDM) - the switch of circulate-border fitness facts without the proprietor's know-how in healthcare from East Africa (EA) increases problems concerning privacy and information safety (Salami, 2022). Emerging technologies, including Artificial Intelligence (AI) and Big Data (Ali, 2025), used to assemble healthcare predictive models, have accelerated the risk of private data exposure. For instance, the Lancet Commission on Diabetes in sub-Saharan Africa developed a predictive model primarily based on machine learning and huge information analytics to estimate the prevalence and incidence of diabetes and its complications in forty-seven African nations. The version utilised statistics from numerous resources, which include demographic and fitness surveys, family income and expenditure surveys, country-wide health bills, and hospital checks, to estimate the burden of diabetes and its financial impact for the period 2015-2030 (Atun et al., 2017).

Data has become a crucial resource for market intelligence and research in product development, but cybercriminals misuse a significant portion of it for financial gain. Transferring personal fitness information across borders increases the risk of data breaches and unauthorised access, particularly if adequate security measures are not in place (UNCTAD, 2016; Salami, 2022). In EA, many fitness statistics are passively stored in foreign repositories, whereas emerging technologies facilitate data collection and transmission in other instances. Furthermore, AI structures from generation giants utilise photographs and videos to extract facial features, developing virtual representations for contrast, identification, and verification, which increases privacy concerns related to the collection, use, and processing of this sensitive data (ÜNVER, 2024). For example,

IBM's Watson Health is a cognitive computing platform that uses AI and massive data analytics to provide insights and solutions for healthcare challenges. The platform has partnered with several African organisations, including the Alliance for a Green Revolution in Africa (AGRA) and the Africa Centres for Disease Control and Prevention (Africa CDC), to acquire and examine records on agriculture, health, and disease outbreaks. The data is employed to improve food security, civic well-being and swiftness to pandemics, yet might elevate ethical and criminal challenges of the information possession, consent and control (IBM, 2021). The study will make an important evaluation on PDM in EA considering the current data protection regulations.

The virtual world is expanding, and security is required to protect the personal health data with the objectives of delivering human dignity, safety, and autonomy. However, in third world countries such as those in EA, deficiency of infrastructure, resources and incentives, and the profits received by domestic actors involved in data collection and management would work against healthcare professionals. In turn, the necessity to rely on international donors made many countries in the region open to foreign influence, and it can be a danger of most of the sensitive information ending in foreign hands. Dependency relationships create unequal power relations that disempower the region to enforce data protection laws.

The problem is worsened by the appearance of new technologies because it becomes even harder to make sure that health data is provided with appropriate protection. Consequently, the burden falls on multinational health Non-Governmental Organisations (NGOs) to collect and utilise health data effectively. The risks of PDM's lack of expertise to track large tech firms' activities also put some countries at risk, as do cyberattacks or other unknown criminals hoping to gain by accessing such information. As an example, the International Network for the Demographic Evaluation of Populations and Their Health (INDEPTH) is a source of the most reliable and comparable data about health research and policymaking in low- and middle-income countries, including Eastern Africa (Herbst et al., 2021). The organisation, like most NGOs, is primarily financed by multinational corporations.

Furthermore, the lack of adequate data safety laws and regulations in EA exposes customers' records to potential misuse, abuse, or exploitation by third parties, including governments, agencies, or hackers (ÜNVER, 2024). This study, consequently, seeks to shed more light on how to mitigate those increasing issues and ensure that fact transfer in EA is conducted in a transparent, moral, and responsible way. The observation contributes to the literature on statistics protection and Transborder Data Flow (TDF) in EA, providing empirical proof and insights on the drivers, styles and influences of PDM. The paper presents suggestions on exceptional practices for boosting information safety and privacy within the region, specifically regarding AI and other emerging technologies.

This study aims to examine the development of a formalised ethical policy framework for cross-border health data transfer systems, ensuring the privacy and security of residents' health information and the implications for data protection and governance within the region. The study examines the following factors of PDM:

- The drivers and motivations behind PDM, consisting of the call for data through overseas entities, the dearth of facts infrastructure and assets in Africa, and the incentives and benefits for local actors involved in PDM.

- The patterns and tendencies of PDM, such as the kinds and sources of statistics amassed, the locations and recipients of information, the techniques and technologies used for records transfer, and the frequency and extent of information flows.
- The effects and consequences of PDM, the potential dangers and harms for customers' privacy and protection, the criminal and ethical demanding situations and dilemmas for facts protection and governance, and the social and monetary implications for information sovereignty and development in Africa.

This study, therefore, investigates the phenomenon of PDM in EA. PDM in this context refers to the passive transfer of personal data collected from customers' devices and various assets, facilitated by emerging technologies such as AI, to third-party individuals and servers located outside the premises. There are hundreds of aid agencies in the region, all of which operate within the healthcare sector. These agencies collect a vast amount of data using numerous tools that enable passive data collection, such as AI. The extensive deployment of internet-based platforms and apps utilising AI to deliver various services, including healthcare, education, online shopping, and entertainment. Such apps and platforms usually track users' personal information on their devices and other sensors, cameras, microphones, etc, without their specific agreement or notice. This information will then be transmitted to third-party centres beyond the region, e.g. in Europe or the US, where it may be processed, stored or sold to other parties, each with diverse aims, including advertisement, research, or product development. Such data transfer is highly risky to the privacy and safety of individuals since they have no control over or monitoring how their information is used, shared, or safeguarded by the foreign parties (Andersen, 2019).

This study is designed to shed light on the tendencies and outcomes of PDM in EA with consideration of different aid agencies and people living in the corresponding countries. Observing the analysis is important to understand how donor agencies can access and use the data provided by the AI-enabler platform. It also helps to understand the AI applications to capture and manage the data concerning their humanitarian and developmental activities in the health sector, such as disease surveillance, diagnosis, treatment, and prevention. It also studies correlations between the citizens of these states and online conditions and programs that provide a range of opportunities, such as social networks, studying online, or shopping, and ways their information is collected and transferred across administrative boundaries. The article assesses both the extent and magnitude of PDM in sub-Saharan Africa and its impacts on the rights and interests of the user, such as privacy and security, autonomy and a right to information. The paper also analyses the prevailing and possible legal and policy systems of regulating and safeguarding PDM inside EA. It makes suggestions for improving data management and responsibility in the area.

This study is significant to EA because of the imbalance of power between the region and the Western world caused by its colonial past. The Southern hemisphere World has seen aid as a potent part of the endgame of the Western World. Whenever there is an imbalance of power, some institutions capitalise on this and obtain or gather this information either passively or actively and deploy it in other investments such as the discovery of new compound drugs or attain a competitive edge in the market (Babalola, 2024). In EA, variations in data protection laws exist among the countries and across Africa, consequently creating uneven regulation of TDF. It is found that some African countries have provided data protection legislation due to international ties. However, the legislation may not necessarily refer to TDF. TDF legislation in Africa is also problematic in that there is little clarity or consistency of law, and regional conventions may be unenforceable or not helpful (Babalola, 2024; Mannion, 2021). Decisions made concerning adequacy in Europe, like the EU-US Privacy Shield, also impact data transfers in equal measure

with African countries. Although Africa is still in the process of unifying its regional frameworks on data protection, including TDF, it still has a way to go to overcome its cohesive approach.

Methodology

The study used mixed-method research using both qualitative and quantitative data. The study primarily relies on face-to-face interviews with key informants, including policymakers, employees from donor agencies such as data managers, project coordinators, and IT staff, to gain insights into their TDF practices, challenges, and perspectives on PDM, as well as their relationships with data protection agencies. For citizens, the study employs a stratified random sampling method to select respective samples of online platform users in six EA countries: Kenya, Uganda, Rwanda, Burundi, Tanzania, and South Sudan. The study administers questionnaires to the selected respondents, asking them about their usage patterns, preferences, and attitudes towards online platforms and applications that rely on AI, as well as their awareness and concerns about PDM. The researchers have also used the phone interviews with a subsample of the respondents where a structured interview guide was employed to bring more lengthy responses and views regarding PDM.

Where quantitative data was provided, Statistical Package for the Social Sciences (SPSS) was used to analyse the data. The SPSS is a statistical programme used to conduct descriptive and inferential statistics of quantitative data (Rahayu et al., 2024). The SPSS assisted in manipulation of the data through such commands as cleaning, coding, recoding, transforming and weighting of the data. The SPSS is also applied in the research to accomplish the frequency analysis. The research also includes qualitative records, which were gathered through in-depth interviews with key informants as well as the policymakers, healthcare professionals and information managers of the local and global business firms. The interviews offered informative information on the real-life challenging conditions and ethical predicaments that are related to Passive Data Migration (PDM) in East Africa. Thematic technique of analysing interview facts implies an identification of the most important issues using the coding and categorisation tool (Williams and Moser, 2019). Such qualitative analysis complements the quantitative information obtained in SPSS because it provides a greater insight into the contextual variables affecting records migration practices. The amalgamation of every statistical and qualitative methodology guarantees the comprehensive approach in which not only the broader tendencies and trends are analyzed but the roots and personal experiences of the tendencies are also considered and, therefore, increase the overall strength and dependability of the results.

Results

This part presents open ended and close ended questions analysis presented to the respondents regarding dynamism of Passive Data Migration (PDM) in East Africa, motivation behind this activity, the trend of data flow and data security, privacy and governance. Using a survey of the responses of 48 transcribed interviews, the question that this paper sought to answer is to what extent local healthcare organisations, research agencies and custodians of data are managing, storing and transferring sensitive health information across borders. This part provides the key findings of such a thematic analysis of these transcriptions. The collective results are categorised into three main themes. Each of the themes is disclosed, with attention paid to the ideas expressed by the study participants, which are supported by facts concerning data protection in East Africa. The close-ended questions were summarised using frequency analysis.

Theme 1: Drivers and Motivations Behind Passive Data Migration (PDM)

The causes and drivers of Passive Data Migration in East Africa are complex, with reasons and drivers that are also multidimensional. These drivers are influenced by both external factors external to the region and internal factors related to the region's lack of data infrastructure and data resources (Migration data portal, 2020). Among the reasons that provoke the growth of PDM is also the rising need for external institutions to receive health information (Alotaibi & Federico, 2020). According to the respondents from the open-ended survey questions, healthcare structures, and authorities' branches, the request via overseas research centres and pharmaceutical organisations for access to fitness data is one of the main reasons for the transfer of confidential fitness statistics beyond local borders. These requests are, likely, pushed via the widespread global literature on fitness reputation and the need for information on sickness occurrence, remedy effectiveness, and health hazard patterns in East Africa.

One of the respondents in Kenya said: "*To track disease outbreaks, various international organisations, including the CDC, require our data so that they can accomplish that objective*." These kinds of organisations are likely to invest in some health programs in the area, and this aspect means that data sharing is one of the major features of this collaboration.*" In the same way, a Tanzanian participant responded: Foreign institutions require information to conduct international studies on diseases like HIV and malaria. They provide financial support and technical support, and this is the reason why local healthcare providers have good reasons to share their data."*

The above responses shows that the external pressure creates an atmosphere in which it is almost impossible not to share data, with local institutions viewing the prospect of a higher budget and increased strength. Similarly, Li et al. (2021) elaborates that health information serve not only as a source of worldwide research, but also as a source of health interventions, such as vaccination campaigns and disease prevention efforts. The second prominent cause of PDM in East Africa is the nonexistence of local data infrastructure. Several of the respondents referred to inadequate data storage and processing facilities at the regional institutions as one of the factors contributing to the situation, which they considered as a motivation to give up on using external-based platforms. The report of Africa (2024) explains that the research institutions and healthcare providers within East Africa have difficulties storing and processing the huge volumes of health data securely.

One of the Uganda data managers said, "*We do not have the infrastructure here to store the data securely. It is not only cheaper but easier for us to store it in an external server because we cannot develop our data centres."*

The above response shows that the lack of such infrastructure limits the ability to analyse the data and monitor health surveillance in real time, and organisations need to outsource the entire set of responsibilities to other organisations overseas, too. Data migration is therefore a necessity when there are few choices within the local area. One of the key drivers was also mentioned as being the motivation of the local actor in PDM. Research by Hussein (2021) states that data migration is an operation that local medical facilities, data managers, and researchers often perform, with the help of international agencies, by providing them with funding and technology. Most of the respondents expressed that entering a data sharing agreement with a foreign body can come with funds for health programs and the availability of resources to improve the local health facilities.

One of the respondents of a Kenyan research facility reported: *"We receive funding and technical resources when we share data with international partners. This helps us continue our work on local health issues."* Another respondent from Mozambique shared: *"Without these external partnerships, we would not have the resources to support our health initiatives. The data sharing*

helps us maintain our programs."
In this respect, the profit of local actors in participating in PDM is determined by financial benefits and the associated capacity building introduced through international partnerships (Akbarnezhad Nesheli, 2023). However, it also implies that local organisations might prioritise facilitating options on the outside over classifications of data justice and preservation, which, in the long run, might be detrimental to data protection in the area.

Theme 2: Patterns and Trends of PDM
The theme focuses on the trends and patterns of Passive Data Migration (PDM) data, including the type of data being collected, methods for transferring the data, and where health data is delivered. The paper established that data migration has become a widespread phenomenon in the area. Still, there exist profound differences in the way data is managed, transferred, and where it is sent.
The information gathered in East Africa primarily falls under the category of personal health data, including medical history, clinical diagnoses, demographic factors, and treatment plans. Most data gathering occurs in a medical environment, including hospitals, clinics, and research studies, most of which were reported by most respondents.
One respondent from a Ugandan hospital described: *"We gather information on HIV patients, how they respond to the treatment, and their care regimens. This information is usually transferred to international organisations to do research."* Another respondent from a Kenyan NGO noted: *"We also gather statistics on maternal health and family planning, and we can report on infant mortality, reporting the same to our international partners in a bid to facilitate global health efforts."*
This health information is typically gathered through surveys, clinical research efforts, and health evaluations conducted by the state and non-governmental research institutes. The data have several applications which may be used in research, policy development, and program monitoring.
The exchange of health data has been managed in several ways; nonetheless, the most common technologies applied during the information transfer were cloud-based services and secure file transfer protocols (SFTP) (Mehrtak et al., 2021). Encryption of data was widespread to preserve security in case of transmission. The research respondents also highlighted the need to use safe systems in transmitting health information to their international partners to minimize chances of being exposed to theft, malpractices or unauthorized access to health information.
A respondent in one of the Tanzanian hospitals said: *"We have cloud storage where data is shared with our international partners through encrypted storage. This would be to make sure that the data is secured when it is in transit but again, we are worried about its security when it gets out of our country."*
This was not preventable by encrypting data and making use of secure rings or channels but posed a question of ineffective protection of health information transferred abroad, particularly, the likelihood of the non-compliance of the data centres located outside of the government with the local data protection statutes (Chan et al., 2024).
In the study, the main target of East African health data research was found to be North America, Europe, and international health agencies. The US, UK, and Canada topped the countries with the most data transfer destinations. In contrast, international organisations such as the World Health Organisation (WHO) and the Centres for Disease Control and Prevention (CDC) were individually mentioned or held the first position (Lyu & Luli, 2021). Such organisations are likely to need data on global health research and policy formulation.
One respondent from a Kenyan research organisation noted: *"The vast majority of the data we are*

receiving is also sent over to research partners either in the US or Europe, where they have the better infrastructure and analytic resources to process the data." The responses showed that transfers of data usually benefit international partners to a greater degree than local health systems, due to a lack of required infrastructure and resources, often have no use for the transferred data after it is received.

Theme 3: Impacts and Consequences of PDM

The consequences of Passive Data Migration and its effects on the process were frequently discussed during the interview sessions. The main effects entailed privacy threats, legal aspects, and a general impact on data sovereignty and regional growth (Fischer, 2023).

After transferring sensitive health information to other countries, the respondents in this study identified the privacy and confidentiality of such information as the most significant area of concern. The respondents expressed concerns that the security of information, including the possibility of data leakage and unauthorised access, would compromise the confidentiality of patient information. The majority of respondents concentrated on the challenge of ensuring data protection once it is given to foreign servers or cloud-based applications.

A data manager from Uganda explained, *"Once they put our data out of the country, we cannot have control over it. We may use encrypted platforms, but there are always some risks of data breaches, and they may appear in particular when the data is stored in a jurisdiction that lacks effective privacy protection."*

Another major issue, as expressed by the respondents, was the legal vacuum that exists when transferring data across borders. Respondents noted that most of the time, there is a compromised informed consent when transmitting health information abroad, hence leading to ethical dilemmas. Other respondents further indicated that the question of data ownership is complicated in the sense that local stakeholders can hardly reclaim the data after it has crossed international boundaries.

A Kenyan respondent reported: *We have difficulty ensuring that patients are aware of where their data is being sent and how it will be used once it is no longer under the jurisdiction of a country. It is one of the profound ethical issues."*

Commercialisation of health information was also cited as one of the problem factors. Other respondents complained that some information shared with their fellow countries is sometimes utilised in profit-making research, whereby there is no precise benefit to the surrounding community.

The problem of data sovereignty has become a vital issue. The most troubled respondents expressed concern that the East African countries would lose the control over their data property, and this can be long term implications on the growth in the region.

According to one employee of healthcare in Tanzania, our data sovereignty must be protected. The health information should not be entrusted to a third party. It ought to affect us on the local level and not only that of the international community.*"*

The results of this research give a vivid outlook of the driving forces, trends, and influences of Passive Data Migration in East Africa. According to the survey by Kaya and Shahid (2025), the practice depends on the international attraction towards the existence of health data and the absence of it in the local infrastructure. Nevertheless, the privacy and legal side of the practice and the issues of data sovereignty should be taken seriously. The article observes that an official ethical policy procedure must be in place to govern the cross-border health data transfer and makes sure that health data of citizens is processed in a manner that maintains their privacy and security.

Quantitative Analysis

The close ended questions focused on decision-making involving vulnerable health data, data confidentiality, as well as the presence of Passive Data Migration (PDM) in East Africa. Using frequency analysis, the degree of awareness about the issue of information security and the perceived sensitivity of fitness-related data were summarised.

Types of Sensitive Health Information

Figure 1 differentiates the types of fitness-related facts which are regarded as "sensitive" among the members. The most sensitive health facts, according to a large percentage of the respondents, were health facilities (85.4%), clinical diagnoses (10.4%) and mental health status (4.2%). The enormous issue involving sanatoriums indicates that there is a very serious concern in terms of clinics and the confidentiality of such figures. Nonetheless, not as invasive as clinical diagnoses, yet just as important in healthcare decision-making, clinical diagnoses are needed.

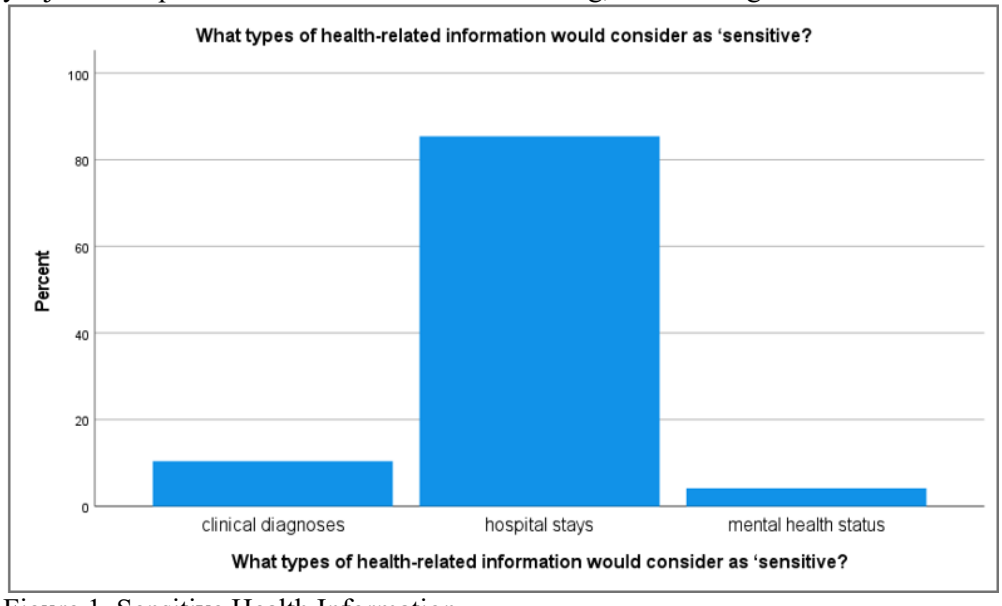

Figure 1. Sensitive Health Information

What Makes Certain Health Information Sensitive

Figure 2 shows how respondents define what makes health records sensitive, emphasising three classes: no precise distinction (4.2%), various tiers of sensitivity (83.3%), and the requirement for better sensitivity (12.5%). A dominant 83.3% of respondents agree that fitness facts have exceptional ranges of sensitivity, which is crucial for tailoring privacy protections accordingly. Some fitness records, including diagnostic records or remedy records, can also require stricter safeguards, whilst others might be less sensitive. The 12.5% who see a need for extra tiers of sensitivity may refer to cases in which people's private health statistics might be exposed to misuse if no longer closely monitored. This differentiation within the notion of sensitivity suggests that healthcare data should no longer be considered as a monolithic entity but as varying statistical types requiring exceptional ranges of protection, from stringent policies to lighter oversight.

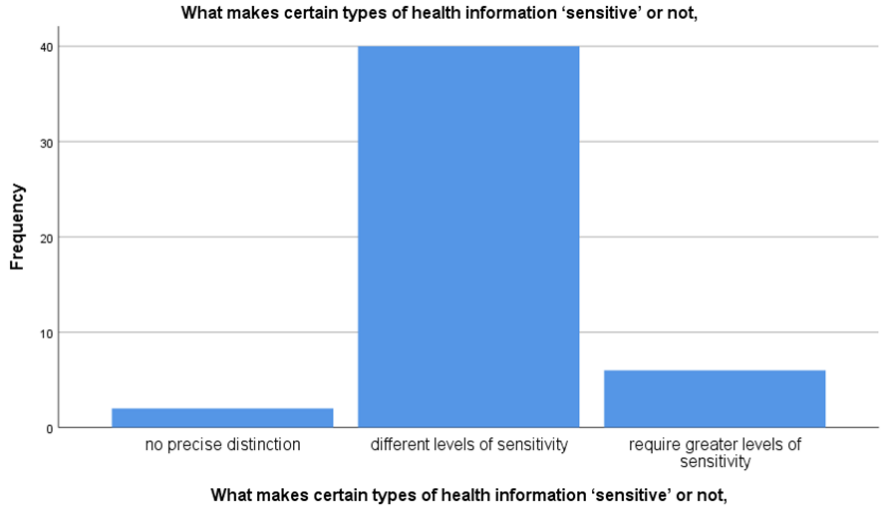

Figure 2. Certain Health Information Sensitive

How Health Information Contrasts with Potentially Sensitive Non-Health Data

Figure 3 explains how non-health information that can be defined as sensitive is viewed against health data. A good proportion of respondents, 68.8% cited financial bank statements as a major non-health data issue, whereas health data in mobile apps or wearable devices was noted by 22.9%. The significant discrepancies between economic and health data from digital tools can indicate a larger societal issue of financial privacy and identity theft. However, 22.9% who recognise the possibility of health information being collected using mobile applications or wearable gadgets suggest that an awakening has occurred around the dangers of newer technologies. The more people use such tools to monitor their health, the greater the risk that their privacy will be compromised. These opposing positions regarding the sensitivity of non- health and health data suggest that new technologies should be regulated with caution to protect their users' privacy and data safety.

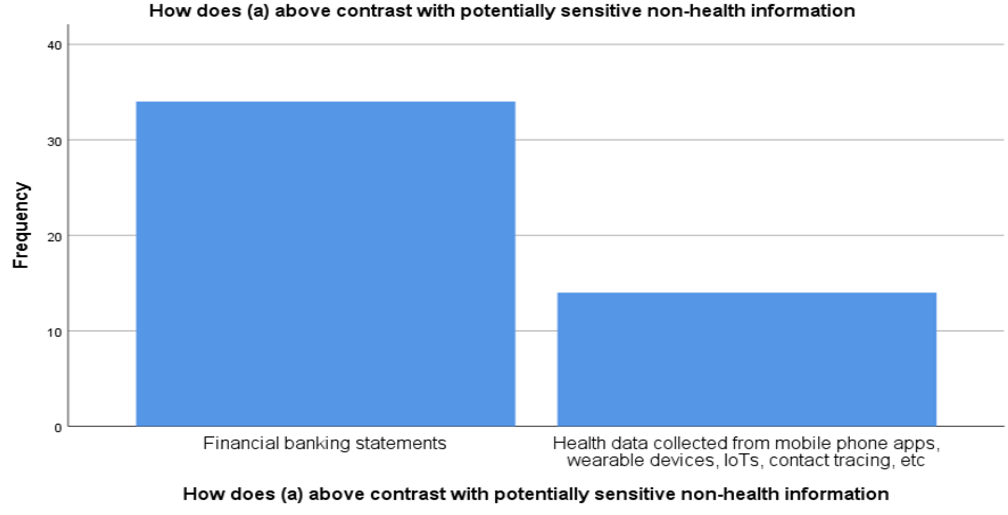

Figure 3. Health Information Contrasts with Potentially Sensitive Non-Health Data

Views on Sensitive Health Information in International Contexts

Figure 4 presents the attitudes of the respondents regarding ethical considerations of the disclosure of their sensitive health records to foreign partners. The information reflects a wide range of views on the issue, with the most significant percentage (68.8%) holding the opinion that health information should be restricted in certain global situations. Only a smaller percentage (8.3%) had apprehension of cloud across research involving international studies where data is open to collaborators in the industry, and only 2.1 % had concerns about the commercialisation of health data. This graph illustrates the prevalence of the contention that there is limited trust in how health data may be utilised beyond national boundaries, especially in research. This trend highlights the need for well-defined ethical frameworks and policies that prioritise local community interests and align international partnerships with privacy standards.

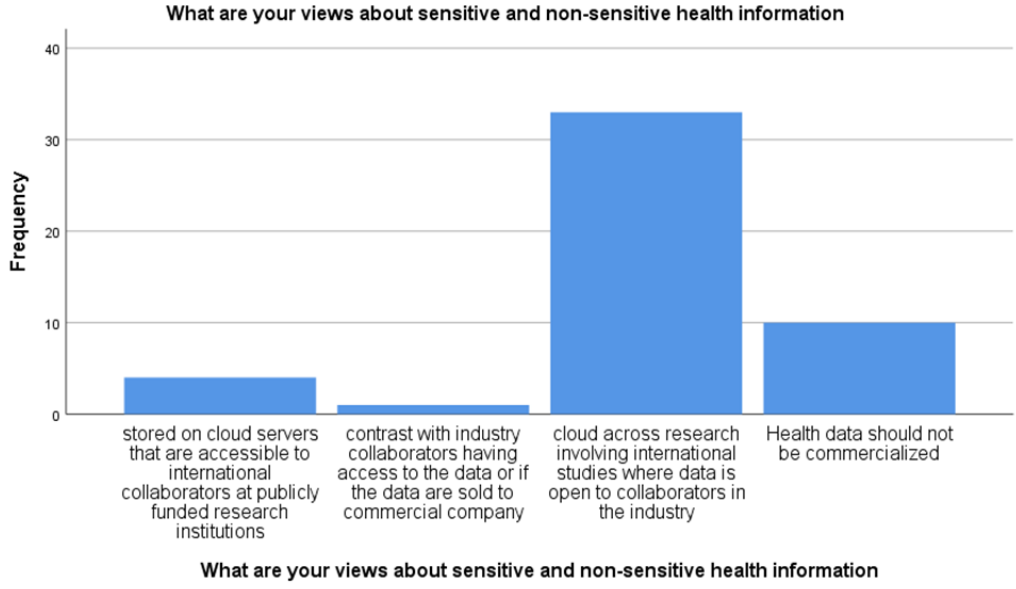

Figure 4. Sensitive Health Information in International Contexts

Importance of Research Purpose or Collaborating Country in Data Sharing

Figure 5 highlights the importance of research and collaboration within the United States in the decision to share sensitive health records across borders. The agreement that the USA or the region of the partners carrying out research is also significant (85.4%), and the purpose of the study is emphasised as another point of determination. The graph shows that the likeliest option to regulate the sharing of information is based on geographical proximity of collaborators, particularly areas like England (41 responses), which implies conformity with jurisdictions which have formulated privacy standards. Moreover, the purpose of the research, especially in the sense of the population health or financial goals, becomes essential to ensure factual safety and ethical conduct.

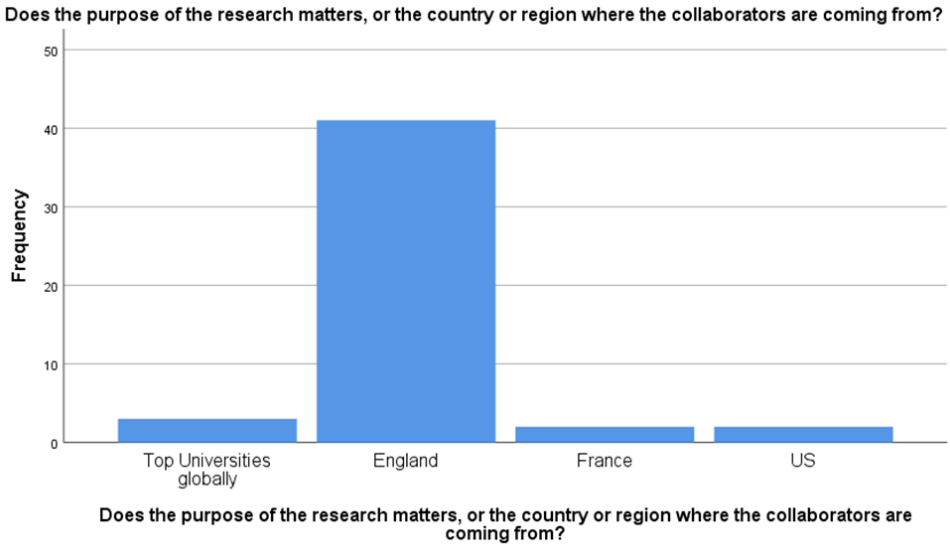

Figure 5. Research Purpose or Collaborating Country in Data Sharing

Conditions for Sharing Sensitive Health Data with International Collaborators

Figure 6 underscores the conditions under which members would come into possession of sensitive information regarding their health and should share it with international partners. The majority felt that sharing information was mostly dependent on situations of public benefit (95.8 per cent), hence the importance of ethical structures that enable information to be used in the public interest. Public advantage should encompass research aimed at enhancing healthcare outcomes or tackling local health challenges, such as disease prevention. These findings replicate an extensive consensus that, while global studies can drive innovation, they must be grounded in the principle of public good, aligning with both local healthcare needs and international ethical standards.

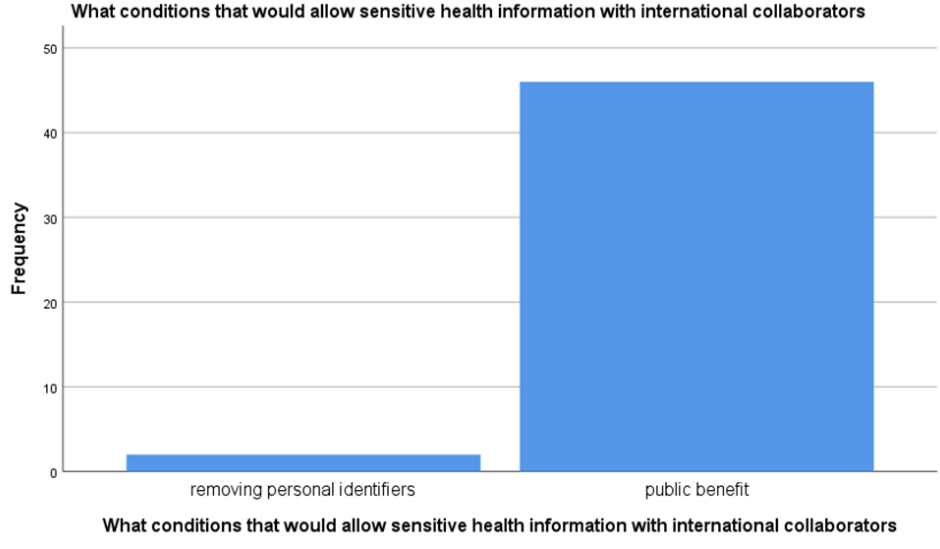

Figure 6. Sharing Sensitive Health Data with International Collaborators

Awareness of Data Regulation and Protection

Figure 7 illustrates participants' recognition of the way fitness information is regulated. The vast majority (87.5%) indicated a high degree of consciousness of statistics safety policies, whilst a small percentage (4.2%) expressed very low consciousness. This heightened awareness of data privacy likely reflects the increasing global concern for data protection and the growing emphasis on health data protection in East Africa, particularly in light of emerging technologies such as AI and cloud computing. However, the minority who mentioned low cognisance may want to factor in gaps in training and education, suggesting a need for similar tasks to elevate awareness about records protection legal guidelines. The high level of awareness among respondents indicates that, despite the availability of comprehensive information, ongoing efforts to enhance this knowledge and address gaps in law and enforcement are crucial for ensuring comprehensive protection for sensitive health information in the vicinity.

Figure 7. Awareness of Data Regulation and Protection

Frequency of Passive Data Migration in Work or Business Activities

Figure 8 demonstrates the rate of interaction of participants in the sports that cause Passive Data Migration (PDM) at work or within their business. Majestic 72.9 per cent were found to have been engaged in it daily, 22.9 per cent engaged in it every week, and 4.2 per cent occasionally engaged in it. The overmuch expediency of PDM activity demonstrates the transfer of health information through international borders under frequent transfer, as well as in many cases without the appreciation of the local stakeholders and without their control. This clarifies the essential importance of additional tight records management and regulations of international data movements.

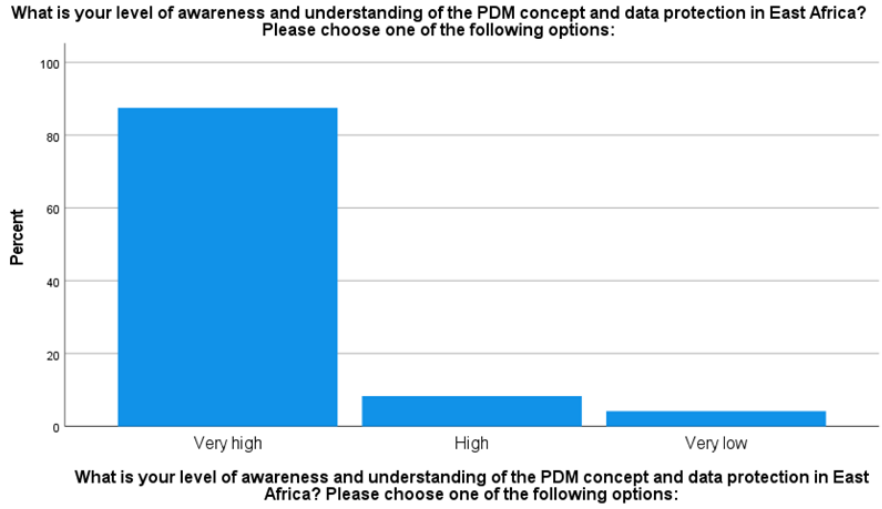

Figure 8. Passive Data Migration in Work or Business Activities frequency

Frequency of Activities Resulting in PDM

Figure 9 shows the frequency of activities that result in Passive Data Migration (PDM) in activities in work or commercial enterprises. Most of the respondents (approximately 72.9) state that they perform PDM activities daily, which implies that there are frequent flows of border records. The proportion of people experiencing PDM on a weekly basis is already lower (22.9%), which points to normal levels though with significantly lower information migration. PDM only occurs now and then with only 4.2% of records indicating its occurrence among a small group. The numbers indicate that the PDM is a routine practice within numerous industries, and the issue of data protection and privacy concern is present because the rates of information cross- border security are too high.

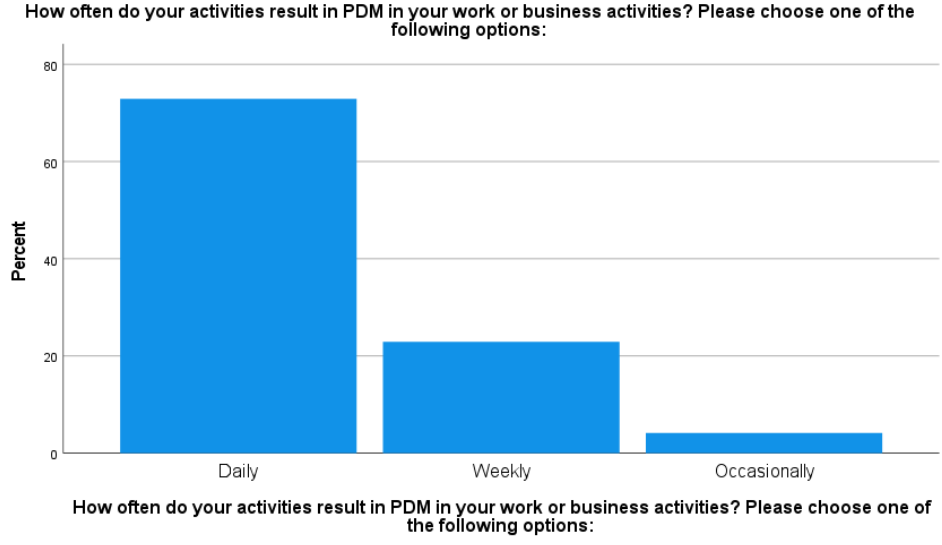

Figure 9. Activities Resulting in PDM frequency

Discussion

This article explores the phenomenon of undertaking Passive Data Migration (PDM) in East Africa, with a focus on trans-boundary data mobility. The first objective revealed that complex and multifaceted approaches in which PDM is positioned, the observable traits in statistical migration, and the far-reaching scope of factors that should not be underestimated, including privacy, security, data sovereignty, and governance. The needs of external users of the data, the absence of local data infrastructure, and the monetary incentives being paid to local actors to enter cross-border data sharing are only some of the forces at the origin of PDM as identified in the study. Similarly, Arinze's (2024) findings explained that the facts go to the global establishments, research institutions, and drug companies, as the world is in widespread need of health statistics in East Africa. The trends of PDM reflect the patterns of the form of the collected information, the data transfer methods, and the mainstreams of transferring health data to that side, as explained in the report of the World Health Organisation (2023). In the meantime, the results of Chiruvella and Guddati (2021) also show that the implications of PDM can cause certain critical issues regarding the safety and privacy of sensitive health data, ethical implications of the data ownership, and regulatory legislation related to transferring data to foreign locations.

In the second objective of the study, the results presented are to reinforce the importance of information on the health of East Africa in undertaking health-related research on a global scale, particularly in the domain of Epidemic diseases such as HIV, malaria, and tuberculosis, where the region is overrepresented. A study conducted by Bradford et al. (2020) asserts that the external requirements of health-related data of international organisations, research organisations, and pharmaceutical companies are perhaps among the most influential forces of Passive Data Migration (PDM). As depicted in the findings, foreign partners typically require extensive data sets from East Africa to inform their studies and community health projects. Doble et al. (2023) explain that in most cases, these international organisations offer funds and technical support in return for gaining access to data that are considered crucial by local organisations towards the sustainability of their health programs.

Bhuiyan et al.'s (2024) findings also revealed that the same pressure is exacerbated by the fact that several diseases common in East Africa are not widely investigated in other regions of the world; hence, local statistics are invaluable to global health researchers. Nevertheless, this outside demand also demonstrates some serious moral and administrative issues. Despite the positive aspects of PDM, such as financing and resources, the transfer of data to other countries is problematic due to the inability to control it locally. Some respondents to the research expressed concern when it revealed the disempowerment of local institutions, particularly in managing the potential data assets generated in East Africa. Laws governing health data that are moved out of the country are most likely to differ from local data protection regulations (Chan et al., 2024). This fact not only exposes the data to a security threat, but it also raises concerns about the exploitation of local metal resources for foreign benefit.

It is not easy to have an independent system of health statistics in East African nations because of their dependence on foreign investment and data-sharing agreements. As seen in the reports by Ali et al. (2024), the region is already very vulnerable because it cannot deal with or store sensitive health data due to the lack of sufficient infrastructure in the area, making it more necessary to establish more advanced local data governance systems. Infrastructure deficit is another issue that led to PDM, according to the study findings. Mehrtak et al. (2021) also identified that the vast amounts of data generated by healthcare providers that they cannot handle and store due to a lack of necessary infrastructure and financial resources are often rerouted to other institutions. As stated

by the respondents consulted during the research, many of the East African institutions are forced to utilise of third-party cloud computing services and external data centres when it comes to storing sensitive health information.

The only option that seems to be available for securely storing large amounts of data is the external solutions." However, local actors may require the convenience of external cloud platforms, as well as the level of control and security that these platforms do not provide. The problem is especially concerning when sensitive health information is stored in locations with fewer data protection regulations. Furthermore, West Africa's reliance on patron structures hinders the improvement of its fitness records structures and technology, perpetuating the disadvantageous cycle of outsourcing (Sulaiman Muhammad Musa et al., 2023). Consequently, the global information system often leaves East African countries in a secondary position, where their natural resources are frequently exploited without sufficient returns accruing to the local communities.

The third objective of the study was that PDM is financially advantageous, which is one of the determinants as to why local actors may be interested in engaging in it, as the survey establishes. The respondents claimed that the health facilities, research centres, and data handlers in the country collaborate regularly with aid agencies, technical resource providers, and capacity-building agencies in other nations to obtain the finances to do their jobs and to enhance service delivery to the community. These findings align with Nyawira et al. (2022) results that incentives are required in an area where healthcare programs are already poorly funded and where not much money is available to invest in research and data maintenance. The financial incentives offered by the global institutions yield a twofold impact, as they increase the willingness of the actors in the locality to disseminate their data, but they pose an ethical issue to the privacy, ownership, and security of data. The economic impact of the release of sensitive health information according to the Cascini et al. (2024) is expensive; there is little payoff and even local actors, which struggle to obtain funding, do not even consider the economic effects such a decision will have when making their choices.

This may lead to misuse of the data with the help of which the information gathered during the conduct of the research is commercialised without consulting the locals or providing them with real compensation. The forces require determining a new balance of the PDM system, where the economic sustainable growth would be balanced with practical data protection methods that would not violate the life interests and rights of indigenous communities. Otherwise, PDM may be the tool of evil as well as liberation. As identified in the study, the most frequent forms of health data found in East Africa are personal health records, diagnostic outcomes, patient treatment histories, and demographic data. This information is accumulated through the conduct of medical trials, health campaigns, vaccination campaigns, and disease surveillance. Most respondents stated that such record sets are essential for monitoring disease developments and developing regulations for public health improvement. However, Hummel et al.'s (2021) findings revealed that the migration of such information outside a country is quite elaborate because of concerns over data sovereignty and local ownership. Data sovereignty concerns aim to limit the extent to which data from local actors is used in methods and places beyond their control.

Regarding the mode of information transfer, the research indicated that cloud-based sites and digital switch tactics (Secure File Transfer Protocol (SFTP) and multi-link computerised storage in encrypted form) were standard. Although such procedures offer some security, they also come with a series of challenges. One of the main issues raised by a significant number of respondents was the specific risk that the data would lose its security once it was transferred to foreign cloud platforms, thereby becoming vulnerable to cyberattacks, unauthorised access, or leakage. Besides, the opacity

with which foreign parties operate this information, in most cases beyond the scope of East African jurisdiction over data protection, has cast doubts on the responsibility of the ultimate handlers of such details (Bor & Koech, 2023). Although security in information transfer, through encryption and secure transmission channels, can mitigate the impact of information transmission risk, it does not guarantee complete information security on foreign servers.

This study's main strength is a comprehensive analysis of Passive Data Migration (PDM) in East Africa, specialising in its drivers, patterns, and influences on information privacy, security, and sovereignty. A most important aspect of this study lies in its empirical technique, incorporating qualitative records accrued from key informants across more than one international location. By inspecting nearby and worldwide views, the study provided a balanced view of the moral and practical challenges posed by PDM in East Africa.

The most significant issue identified by the study is the privacy and security risks associated with the cross-border transfer of health data. Although cloud storage techniques and statistical encryption are used, sensitive fitness records might also still be vulnerable to breaches, hacks, and unauthorised access (Nemec Zlatolas et al., 2024). These issues had been raised by contributors, who stated that statistics safety policies connected to storing patient fitness facts on non-neighbourhood systems might not be equal to the local data protection policies that apply within a region, thereby risking patient privacy. The digital world is rapidly evolving, and cyber threats are becoming increasingly sophisticated; therefore, information security should be a top priority when transferring data across borders (Bolatbekkyzy, 2024). The research additionally highlights numerous demanding situations associated with law and ethics that pertain to PDM. There were limitations related to the study as it used self-reported data, which could affect the results due to recall or social desirability bias. The access to secure health data repositories in East Africa was a limitation to the scope of quantitative data. In addition to this, cross-sectional design did not focus on long-term patterns, and the findings may not be applicable to all countries in the region because not all the countries in the region have identical infrastructure and systems of data protection.

Conclusion

The East African issue of Passive Data Migration of data (PDM) is very challenging in terms of privacy, data safety, and governance and especially within the healthcare industry. The more the health information of the area is transferred abroad, where in most cases, the facts or consent of the citizens are not taken into consideration, the more the chances of abuse, breaches, and statistical sovereignty are at risk. However, despite these positive aspects of the exchanges of these records such as investments in health programs and partnerships in conducting global studies the region is susceptible because of lack of proper infrastructure, ability to enforce the law on information protection, and lack of a proper regulatory framework. The quote highlights how the East African countries desperately need ownership of their fitness data and that the use should be mutually beneficial to the local communities and immoral concepts. The facts will still be used against the area without more powerful local guidance and with a better records administration system, which probably will ruin its sovereignty and development ambitions.

Recommendation

To address the risks associated with Passive Data Migration in East Africa, several measures can be put in place. These legal provisions should offer clear guidelines on this consent, ownership on the data and when such data can be transferred to distant places. The cooperation between the regions will also be enhanced to establish a single model of data protection, where each country within the

region is subject to the same standards (Mukuki and Assenga, 2024). The implications of this study as far as both policy and exercise in East Africa is concerned are far reaching. The widespread rate of Passive Data Migration also points to the immediate need of more powerful records safety frames and the investment of infrastructure in the region. To reduce dependence on foreign statistics centres which in many cases are outside the control of neighbourhood regulatory systems, countries in East Africa need to put a great emphasis on developing neighbourhood records management and processing talents. The observation also highlights the importance of improving the awareness of people regarding the risks related to information sharing and how the increasing prevalence of technology, such as AI, contributes to these issues. Governments, non-governmental organizations, and other stakeholders must collaborate to formulate wholesome and integrated legal frameworks of cross-border information flows ensuring that the merits of global health studies are not at the expense of local facts sovereignty. Also, the observation made by Abiodun (2025) suggests that the governments should invest in the development of robust neighbourhood statistics that will reduce the dependency on external cloud services and data centres. This could enable the healthcare professionals and researchers to manage and save sensitive health data safely in the region. First, as Wanekeya (2023) says, East African international places require the establishment of elaborate records protection legal frameworks that address specifically cross-border records flows. The local stakeholders, such as healthcare workers and data managers, are also crucial in building capacity to ensure better data security and avoid misuse (Majebi et al., 2024). Finally, transparency and accountability in the agreements of sharing statistics should be considered in the first place, and strict moral principles regarding the way health statistics are applied and to what purposes (Alshar'e et al., 2024). These actions may help to protect the privacy and safety of the records of people and create a more just and responsible attitude to the control of data in East Africa.

Future work

The literature ought to be used in the future to examine the effectiveness of the new statistical safety legal regulations and frameworks in East Africa. In addition, the research must also look into how new technologies, including blockchain, can be used to protect data and ensure greater openness in the process of data sharing. Research such as the one by Khan (2025) should examine the actual international impact of such policies on cross-border information migration and the degree to which it addresses the issue of privacy concern. The review of the general awareness and attitude toward Passive Data Migration can also be considered another place one can apply destiny painting, including the ways people learn about the risks of data privacy and utilizing AI in healthcare (Aldossari, 2023). It is also necessary to consider how East African countries should work in closer cooperation with the international companies so that the information-sharing contracts would be more focused on the local interests and the outcomes of the population health. Lastly, Sampath and Tregenna's (2023) study comparing the moral implications of fact sovereignty and its effect on regional development desires could offer valuable insights into how East African nations can protect their facts while contributing to global research efforts.

Acknowledgement

I want to express my sincere gratitude to all people who contributed to the finishing touch of this look. I would like to thank my co-author Mr. Ben Mukalama who helped in the collection of data. I might want to thank the respondents from study establishments, healthcare systems, and government branches in East Africa for their worthwhile insights and cooperation. I also acknowledge the help of numerous global companies, whose statistics, sharing agreements, and investment facilitated the research technique. Lastly, I wish to extend my appreciation to my

academic mentors and associates for their continuous steering and encouragement throughout this study including Prof. Sekalala, Sharifah and Yureshya.Y.S.Perera – Warwick University, Al Kags and the entire team at Open Institute

Declaration

I hereby claim that the study's paintings offered in this paper are original and have not been submitted for any other degree or publication, and all resources of data, whether primary or secondary, have been duly acknowledged in the references section. The views expressed in this paper are those of the author and no longer necessarily mirror the views of the institutions or companies noted.

Funding Information

The Paper was part of the wider research funded by Welcome Trust UK. Welcome Trust through Warwick University and the University of Nairobi.
Grant REF: 222429/2/1/2

.

References

Abiodun, K., (2025). Digital infrastructure & sustainable data centres investment in Africa: Role of Tier III & Tier IV. Int. J. Multidiscip. Res. Growth Eval. 6(1), 1878–1888.

Africa, H.H., (2024). Assessing Digital Health Infrastructure and Uptake (East Africa) - HealthTech Hub Africa. [online] HealthTech Hub Africa. Available at: https://thehealthtech.org/digital-health-infrastructure-and-uptake [Accessed 30 July 2025].

Akbarnezhad Nesheli, S., (2023). Key lesson regarding project delivery model (PDM) in mega suspension bridge projects, case study: PPP in 1915Çanakkale Bridge Project.

Aldossari, M., (2023). Participants' perceptions of privacy and data sharing regarding health-related data using artificial intelligence. Asian J. Sci. Appl. Technol. 12(2), 6–12.

Ali, N.A.D., Dhamanti, I., Notobroto, H.B., Hidajah, A.C., Anas, (2024). Mapping vulnerability to potential crisis events in Surabaya City: A GIS-based approach. F1000Research 13, 465. https://doi.org/10.12688/f1000research.145182.2

Ali, H. (2025). The influence of machine learning on consumer decision making patterns in Germany: The mediating role of AI recommendation systems for achieving sales and customer satisfaction. AJBMSS-Advance Journal of Business Management and Social Sciences, 1(1).

Alotaibi, Y., Federico, F., (2020). The impact of health information technology on patient safety. Saudi Med. J. 38(12), 1173–1180. https://doi.org/10.15537/smj.2017.12.20631

Alshar'e, M., Abuhmaidan, K., Ahmed, F.Y., Abualkishik, A., Al-Bahri, M., Yousif, J.H., (2024). Assessing blockchain's role in healthcare security: a comprehensive review. Informatica 48(22).

Andersen, (2019). Artificial intelligence in international development: Avoiding ethical pitfalls. [online] Available at: https://openurl.ebsco.com/... [Accessed 30 July 2025].

Arinze, E.D., (2024). A thorough examination of open data initiatives in East Africa, focusing on how they improve the accessibility of data.

Atun, R., Davies, J.I., Gal, E.A., Bärnighausen, T., Beran, D., Kengne, A.P., Levitt, N.S., Mangugu, F., Nyirenda, M.J., Ogle, G.D., Ramaiya, K., (2017). Diabetes in Sub-Saharan Africa: From clinical care to health policy. Lancet Diabetes Endocrinol. 5(8), 622–667.

Babalola, (2024). Transborder flow of personal data (TDF) in Africa: Stocktaking the ills and gains of a divergently regulated business mechanism. Comput. Law Secur. Rev. 52, 105940. https://doi.org/10.1016/j.clsr.2024.105940

Bhuiyan, M.A., Galdes, N., Cuschieri, S., Hu, P., (2024). A comparative systematic review of risk factors, prevalence, and challenges contributing to non-communicable diseases in South Asia, Africa, and the Caribbean. J. Health Popul. Nutr. 43(1). https://doi.org/10.1186/s41043-024-00607-2

Bolatbekkyzy, G., (2024). Legal issues of cross-border data transfer in the era of digital government. J. Digit. Technol. Law 2(2), 286–307.

Bor, S., Koech, N.C., (2023). Balancing human rights and the use of artificial intelligence in border security in Africa. J. Intell. Prop. Inf. Tech. L. 3, 77.

Bradford, L., Aboy, M., Liddell, K., (2020). International transfers of health data between the EU and USA: A sector-specific approach for the USA to ensure an 'adequate' level of protection. J. Law Biosci. 7(1).

https://doi.org/10.1093/jlb/lsaa055
Cascini, F., Pantovic, A., Al-Ajlouni, Y.A., Puleo, V., Maio, L.D., Ricciardi, W., (2024). Health data sharing attitudes towards primary and secondary use of data: A systematic review. EClinicalMedicine 71, 102551. https://doi.org/10.1016/j.eclinm.2024.102551
Chan, H.Y., Toh, H.J., Lysaght, T., (2024). Cross-jurisdictional data transfer in health research: Stakeholder perceptions on the role of law. Asian Bioeth. Rev. 16(4), 663–682. https://doi.org/10.1007/s41649-024-00283-8
Chiruvella, V., Guddati, A.K., (2021). Ethical issues in patient data ownership. Interact. J. Med. Res. 10(2), 1–9. https://doi.org/10.2196/22269
Doble, A., Sheridan, Z., Razavi, A., Wilson, A., Okereke, E., (2023). The role of international support programmes in global health security capacity building: A scoping review. PLOS Glob. Public Health 3(4), e0001763. https://doi.org/10.1371/journal.pgph.0001763
Fischer, A., (2023). Data sovereignty and e-governance: The legal implications of national laws on digital government systems. Legal Stud. Digit. Age 2(4), 1–12.
Herbst, K., Juvekar, S., Jasseh, M., Berhane, Y., Chuc, N.T.K., Seeley, J., Collinson, M.A., (2021). Health and demographic surveillance systems in low- and middle-income countries: History, state of the art, and prospects. Glob. Health Action 14(sup1), 1974676.
Hummel, P., Braun, M., Tretter, M., Dabrock, P., (2021). Data sovereignty: A review. Big Data Soc. 8(1), 2053951720982012.
Hussein, A.A., (2021). Data migration needs, strategy, challenges, methodology, categories, risks, and uses with cloud computing, as well as improvements in its use with a proposed model (DMig 1). J. Inf. Secur. 12(1), 79–103. https://doi.org/10.4236/jis.2021.121004
Kaya, M., Shahid, H., (2025). Cross-border data flows and digital sovereignty: Legal dilemmas in transnational governance. Interdiscip. Stud. Soc. Law Polit. 4(2), 219–233.
Khan, M.N.I., (2025). Cross-border data privacy and legal support: A systematic review of international compliance standards and cyber law practices.
Li, L., Novillo-Ortiz, D., Azzopardi-Muscat, N., Kostkova, P., (2021). Digital data sources and their impact on people's health: A systematic review of systematic reviews. Front. Public Health 9, 645260. https://doi.org/10.3389/fpubh.2021.645260
Lyu, J.C., Luli, G.K., (2021). Understanding the public discussion about the Centres for Disease Control and Prevention during the COVID-19 pandemic using Twitter data: Text mining analysis study. J. Med. Internet Res. 23(2), e25108. https://doi.org/10.2196/25108
Majebi, N.L., Adelodun, M.O., Anyanwu, E.C., (2024). Community-based interventions to prevent child abuse and neglect: A policy perspective. Int. J. Eng. Inventions 13(9), 367–374.
Mannion, C., (2021). Data imperialism: The GDPR's disastrous impact on Africa's e-commerce markets. Vand. Law Rev. 53, 685.
Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., Heydari, M., Barzegary, A., Mirzapour, P., Soleymanzadeh, M., Vahedi, F., Mehraeen, E., Dadras, O., (2021). Security challenges and solutions in healthcare cloud computing. J. Med. Life 14(4), 448–461. https://doi.org/10.25122/jml-2021-0100
Migration Data Portal, (2020). Human mobility in Eastern Africa. [online] Available at: https://www.migrationdataportal.org/regional-data-overview/human-mobility-data-eastern-africa [Accessed 30 July 2025].
Mukuki, A., Assenga, A., (2024). Comparative study of data protection legislation frameworks across the East African Community. D4D Hub March 2024–05.
Nemec Zlatolas, L., Welzer, T., Lhotska, L., (2024). Data breaches in healthcare: Security mechanisms for attack mitigation. Clust. Comput. 27(7), 8639–8654.
Nyawira, L., Tsofa, B., Musiega, A., Munywoki, J., Njuguna, R.G., Hanson, K., Mulwa, A., Molyneux, S., Maina, I., Normand, C., Jemutai, J., (2022). Management of human resources for health: Implications for health systems efficiency in Kenya. BMC Health Serv. Res. 22(1), 1046.
Radanliev, P., (2025). Privacy, ethics, transparency, and accountability in AI systems for wearable devices. Front. Digit. Health 7, 1431246.
Rahayu, N.I., Muktiarni, M., Hidayat, Y., (2024). An application of statistical testing: A guide to basic parametric statistics in educational research using SPSS. ASEAN J. Sci. Eng. 4(3), 569–582.
Salami, E., (2022). Implementing the AFCTTA agreement: A case for the harmonisation of data protection law in Africa. J. Afr. Law 66(2), 281–291.
Sampath, P.G., Tregenna, F., (2022). Digital sovereignty: African perspectives. Johannesburg: DSI/NRF South African Research Chair in Industrial Development.

Sulaiman Muhammad Musa, Haruna, U.A., Manirambona, E., Eshun, G., Dalhatu Muhammad Ahmad, D.A.D., Gololo, A.A., Musa, S.S., Abdulkadir, A., Lucero-Prisno, D.E., (2023). Paucity of health data in Africa: An obstacle to digital health implementation and evidence-based practice. Public Health Rev. 44, 1605821. https://doi.org/10.3389/phrs.2023.1605821

UNCTAD, (2016). Data protection regulations and international data flows: Implications for trade and development. [online] Available at: https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf [Accessed 30 July 2025].

Ünver, H.A., (2024). Artificial intelligence and human rights: Using AI as a weapon of repression and its impact on human rights. [online] European Parliament. Available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450_EN.pdf [Accessed 30 July 2025].

Vaughan, M., Adjaye-Gbewonyo, K., Mika, M., (2021). Epidemiological change and chronic disease in sub-Saharan Africa: Social and historical perspectives. UCL Press.

Wanekeya, E., (2023). Effectiveness of domestic data protection laws in African countries: A case study of the data protection law in Kenya.

Williams, M., Moser, T., (2019). The art of coding and thematic exploration in qualitative research. Int. Manag. Rev. 15(1), 45–55.

World Health Organisation, (2023). Data collection tools - WHO. [online] Available at: https://www.who.int/data/data-collection-tools [Accessed 30 July 2025].

.