AI Health Interventions and Data Protection in Africa: A Systematic Review and Policy Analysis of Pandemic Preparedness in Tanzania

Natalie Frigon

Student ID: 101382211

Norman Paterson School of International Affairs, Carleton

INAF5706: Global Health Policy

Dr. Valerie Percival

November 27th, 2025

Word Count: 4734

Introduction

Artificial intelligence (AI) has been rapidly implemented into healthcare systems around the world. The World Health Organization (WHO) defines AI as the ability of algorithms to independently analyze data and make decisions without the guidance of a human (WHO, 2024). AI is a revolutionary force in the healthcare industry and holds the ability to increase the effectiveness and alleviate burdens of healthcare systems, especially in low-to middle-income countries (LMICs) (Ndembi et al., 2025; Panteli et al., 2025). Common AI health interventions include diagnostic tools, health chatbots, triage assistants and pandemic surveillance platforms (Li et al., 2025; Townsend, 2025).

However, the speed of AI implementation has outpaced the development of regulatory structures that protect individuals' data, specifically in the context of AI. This leaves questions of data sovereignty, and how people's data is being protected and whether it can continue to be protected post data breach. These questions are amplified in LMICs, where digital governance is underdeveloped, and where health data is being increasingly collected through mobile technology (Valle-Cruz et al., 2024).

This systematic literature review asks: What does existing literature reveal about the risks of data misuse in AI-enabled health interventions, and what safeguards exist, or are missing, to prevent or mitigate harm post data breach? This review focuses on Sub-Saharan Africa (SSA), where many global health organizations, non-governmental organizations (NGOs), and humanitarian organizations, including Grand Challenges Canada (GCC), operate to support digital health innovation. Within this context, the Republic of Tanzania was selected as a case study as it represents a rapidly digitizing health system with emerging AI initiatives and limited regulatory protection. AI pandemic tracking was selected as a throughline due to the Tanzanian government's recent AI implementation in the nation's health information management system. The purpose of this paper is to build a greater understanding of the various consequences the implementation of AI can have, and what forms of safeguards can be used to prevent privacy breaches.

This paper is organized into four parts. First, it outlines the methodology and search strategy used to review existing research. Second, it presents key themes identified in the literature. Third, it applies these themes to a case study of Tanzania, analysing the country's AI-based pandemic preparedness efforts alongside current Tanzanian data protection policy such as the 2023 Personal Data Protection Act (PDPA), as well as compare it to the European Union's General Data Protection Regulation (GDPR), which is regarded as the gold standard of data protection (Mantelero, 2021). This paper concludes by identifying gaps in current safeguards and outlining areas for future research, specifically focusing on post-leak data protection in AI health interventions.

Background

AI Health Interventions in Sub-Saharan Africa

SSA is currently experiencing a myriad of healthcare challenges due to its large rural population, poor infrastructure, disproportionate burden of illness, low levels of education, and lack of primary care access (Townsend, 2025). It is also an incredibly diverse region that requires community-specific solutions (Ndembi et al., 2025). AI health interventions have shown the ability to increase healthcare efficiency (Sukums et al., 2023). AI technology has already been implemented across Africa; examples include using AI for medical imaging analysis in South Africa (SA), clinician diagnostic support in Tanzania and Ghana, and database analysis for fetal abnormalities in Algeria, Egypt, Malawi, and Uganda (Townsend, 2025). Following the COVID-19 pandemic, AI implementation in healthcare has further accelerated (Sukums et al., 2023).

Tanzania has published two health strategies since 2013: the Tanzania National eHealth Strategy 2013-2018 and the National Digital Health Strategy 2019-2024. The first strategy prioritized building the infrastructure for healthcare transformation, while the latter focused on digital health solutions for pressing challenges (Makulilo et al., 2025). In 2023, Tanzania's first framework for personal data protection came into effect, titled the PDPA (Makulilo et al., 2025). The PDPA created the Personal Data Protection Commission (PDPC) and outlined the clear responsibilities for data controllers and processors, as well as established individual data rights (Makulilo et al., 2025). It broadly defines personal data as any identifiable information, including employment, education, and medical information (PDPA, 2023; Makulilo et al., 2025). It defines sensitive personal data as genetic information, criminal history, data on minors, biometric data, and any information that can reveal one's race, religion, gender, sexual activity, relationships, gender, or philosophy (PDPA, 2023).

Defining concepts

An AI health intervention is a tool that is used to support healthcare systems using machine-learning systems, which includes diagnostic tools, health-tracking applications, disease-monitoring and outbreak detection (Sukums et al., 2023).

This paper refers to multiple forms of data misuse: (1) data poisoning, (2) AI hallucinations, and (3) misinformation. Data poisoning occurs when an unauthorized user accesses an AI model's training data and intentionally manipulates the data to alter the output (Chen & Esmaeilzadeh, 2024). This harmful action may cause incorrect outputs and AI hallucinations (Khalid et al., 2023). An AI hallucination occurs when an AI produces an output as truth, when it is incorrect (Chen & Esmaeilzadeh, 2024). AI-manufactured misinformation in healthcare includes fake sources, clinically harmful advice, and incorrect facts without malicious intent (Bandeira et al., 2025a; Monteith et al., 2024)

Methodology

Search Strategy

This review began with a broad search to identify how AI health interventions have been misused in LMICs. This review first focused on three domains: weaponization, misinformation, and hallucination-related errors. Searches were conducted in Google Scholar, PubMed, BioMed, Scopus, and Science Direct, covering academic and grey literature published from 2015 to November 2025. This temporal scope was selected as machine learning, and AI in pandemic surveillance became more relevant after the 2014-2016 Ebola outbreak. Tanzania was selected as a case study due to its growing digital health infrastructure, and AI pandemic surveillance was selected due to the recent integration of AI in District Health Information Software 2 (DHIS2) for pandemic tracking.

Search terms used in Boolean strings include: “Artificial Intelligence,” AND “Health Data,” AND “Weaponization,” “Artificial Intelligence” AND “Digital Health” AND “Africa,” “Artificial Intelligence” AND “Hallucinations” AND “Health,” “Artificial Intelligence” and “Health Interventions” AND “Misinformation,” “Artificial Intelligence” AND “Digital Health” AND “Tanzania,” "Tanzania" AND "Data Protection" AND "Artificial Intelligence" AND "Health Data," and "Artificial Intelligence" AND "Tanzania" AND "Pandemic Preparedness."

As the search continued, the scope narrowed to Tanzania and pandemic preparedness to reflect this review's case study. Additional targeted searches were conducted due to a lack of literature found in initial searches for pandemic and policy related sources

Inclusion and Exclusion Criteria

The inclusion criteria included English papers, peer-reviewed articles, review papers and book chapters. Exclusion criteria included studies, non-peer-reviewed articles, publications focused on clinical hallucinations, literature centred on social media misinformation, non-English papers, opinion pieces, and non-English papers.

The title search initially identified 119 papers. After removing duplicates, 79 remained. An abstract screen left 43 articles for a full-text review, in which 19 were selected for final analysis. To ensure replicability, the search was repeated using the same terms after initial screening. Four articles were added using a manual search to fill in gaps regarding policy and infectious disease surveillance in Tanzania.

Figure 1

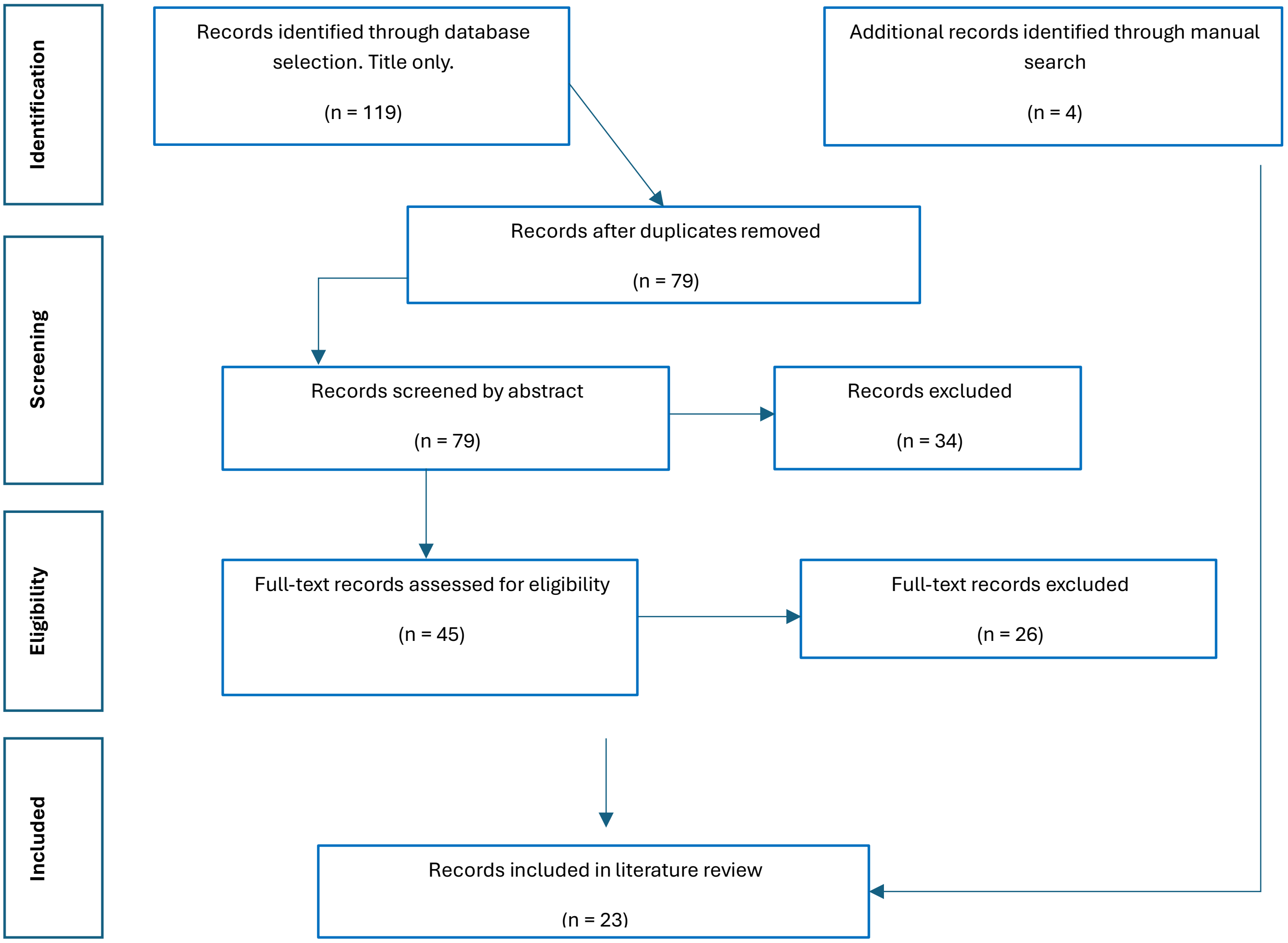
Inclusion Exclusion Criteria

	Included	Excluded
Article Type	Peer Reviewed Policy Papers Press Releases Book Chapters Review Articles	No Access Op-Eds Non-English Non-Peer Reviews Journal Articles Articles on clinical hallucinations and social media misinformation
Methodology	Qualitative	

	Quantitative Mixed Methods	
Geographic Scope	Africa Tanzania Europe (for GDPR comparisons)	Non EU/AU regions
Time Frame	2015 onwards	Pre 2015

Figure 2

Decision Flow


Identification
Screening
Eligibility
Included
Records identified through database selection. Title only.
(n = 119)
Additional records identified through manual search
(n = 4)
Records after duplicates removed
(n = 79)
Records screened by abstract
(n = 79)
Records excluded
(n = 34)
Full-text records assessed for eligibility
(n = 45)
Full-text records excluded
(n = 26)
Records included in literature review
(n = 23)

Results

The literature reviewed highlighted themes of risks to data integrity, including data poisoning, hallucinations, and digital sludge that distort clinical decision-making and public understanding. Due to unrepresentative datasets, there is bias in outputs, which disproportionately impacts marginalized groups. Studies also reveal that there are significant privacy and security vulnerabilities, with rising re-identification, reconstruction, and inference attacks, which are emphasized by the underinvestment in cybersecurity. Finally, structural constraints, such as weak infrastructure, regulatory gaps, and limited education, restrict the effective deployment of AI health interventions in LMICs.

Key Themes

AI Misuse and Data Integrity Risks

Data Poisoning

A key finding is that data is vulnerable to misuse, and integrity is one of the most significant weaknesses in AI health systems. This weakness occurs since AI models depend on large volumes of cleaned, sensitive health data (Chen & Esmaeilzadeh, 2024). When the data used to train an AI model is intentionally manipulated, there are severe consequences that threaten data integrity (Chen & Esmaeilzadeh, 2024; Khalid et al., 2023). This is referred to as data poisoning, which can occur through fabricated patient profiles or altered clinic records, and can change how a model interprets patterns (Chen & Esmaeilzadeh, 2024). Once the database has been contaminated, the model may produce outputs that appear accurate; however, they are misleading or sometimes, completely fabricated. This phenomenon is referred to as AI hallucinations (Chen & Esmaeilzadeh, 2024). Khalid et al. (2023) discuss how data poisoning is a threat to data integrity, as it can create hallucinations and is a critical challenge for AI systems to mitigate

Data Hallucinations

A recent review reported findings from a study showing that the AI dictation tool “Whisper,” used in healthcare settings, produced hallucinations by inserting false text into otherwise accurately transcribed content (Denecke et al., 2025). Although only 1.4 per cent of 13,140 samples contained hallucinations, 40 percent of the hallucinations were deemed harmful, including racist language, violent rhetoric, and fake medications (Denecke et al., 2025). Additionally, S.A.R.A.H., the World Health Organization (WHO) and ChatGPT3.5’s collaborative AI health intervention, found that the model was outputting inaccurate information that went against WHO’s health guidelines (Denecke et al., 2025).

Digital Sludge

The spread of misinformation through AI-generated content has made it difficult for the public to differentiate what is accurate health information and what is false (Bandeira et al., 2025). This difficulty impacts the effectiveness of health interventions. AI has brought an increase in “digital sludge,” which occurs when the internet is flooded with AI-generated content such as deepfakes, misinformation, and social media posts (Bandeira et al., 2025). There is concern that this content is being fed into AI models and therefore modifies the models’ outputs negatively (Bandeira et al., 2025). Additionally, confusion over what is the “right information” can be weaponized by health-harming industries such as alcohol and tobacco companies (Bandeira et al., 2025). These health-harming industries contribute to digital sludge to market their products, shaping AI behaviour (Bandeira et al., 2025). Furthermore, digital sludge can create AI hallucinations, which blur the line between misinformation, which is not intentional, and disinformation, which is then purposefully spread of false information (Bandeira et al., 2025).

Data Bias

Similarly, AI systems can also cause direct harm when they produce biased or inaccurate outputs (Goodman et al., 2023; Mwogosi, 2025a). Standley et al. (2025) discuss this phenomenon in the context of AI health interventions used in African dermatology clinics. Image models trained on primarily lighter-skinned populations performed significantly worse when detecting skin cancer on darker skin (Standley et al., 2025). This example demonstrates how biased training data can lead to harmful or incorrect AI-driven clinical decisions in LMIC contexts. Additionally, Denecke et al. (2025) found that Black patients needing liver transplants were incorrectly delayed since the algorithms falsely overestimated their kidney functions, delaying their transplant priority. Due to the diversity of Africa, it is easy to overlook marginalized groups, which impacts the effectiveness of AI health solutions in the region (Ndembi et al., 2025).

The high resource cost of data collection for AI intervention pushes reliance on datasets that are predominantly sourced from the Global North (Townsend, 2025). This practice produces algorithmic bias and misinformation in the African context, as there is limited data from the region. Since models are trained on available datasets, AI can inherit bias, producing errors and false positives, which impact its accuracy (Valle-Cruz et al., 2024). Goodman et al. (2023) argue that AI interventions are a double-edged sword; they can help prevent outbreaks and be used for epidemic tracking, but they can create or feed into stereotypes about certain groups since they are based on such a small dataset. Townsend (2025) highlights that systemic exclusion of marginalized groups, noting that women in LMICs are frequently not factored into AI model training data, resulting in inequitable, biased outputs and misinformation. Since models are not trained on culturally relevant datasets, there is a risk of AI health interventions reducing culturally significant practices into problematic terms (Townsend, 2025).

Privacy Threats and Security Vulnerabilities

A study by Valle-Cruz et al. (2024) provides an overarching example of how the expansion of AI has presented privacy concerns. Increased AI integration has produced an abundance of avenues through which people can produce data (Valle-Cruz et al., 2024). For example, social media posts, mapping systems, online searches, and even biometric data are being collected from fingerprints, video surveillance, and face identification (Valle-Cruz et al., 2024). The proliferation of data collection points has made it possible for AI models to aggregate information from multiple pathways, raising concerns that this mass available data could be subject to misuse.

Cybersecurity Attacks

The healthcare sector is especially vulnerable to cybersecurity attacks due to the sensitive nature of its data. Khalid et al. (2023) found that from 2018 to 2023, 157.4 million people were impacted by health data breaches. The authors identify three major forms of privacy attacks on AI health datasets: (1) re-identification, (2) reconstruction, and (3) property inference attacks (Khalid et al., 2023). Re-identification or de-identification is harmful as it re-identifies anonymized sensitive health data, exposing the subject's identity and health status (Mwogosi, 2025a). Mwogosi (2025a) found that even if data has been stripped of personal identifiers, AI models can re-identify data when analyzing databases for computations. Reconstruction attacks occur when an unauthorized user rebuilds a raw dataset using accessible non-sensitive information, revealing private data that was originally concealed, once again identifying subjects (Khalid et al., 2023). Lastly, property interference manifests when one analyzes the outcomes of an AI model and, using the outcomes, deduces information that was meant to stay sensitive (Khalid et al., 2023).

Structural and Contextual Constraints in LMICs

Structural Barriers to AI Deployment

LMICs are fundamentally constrained by a range of resource and infrastructural challenges, including a lack of human capital, weak regulations, and unreliable internet and electricity (Naidoo, 2024; Ndembi et al., 2025). These structural issues are highlighted by Africa's vast disparity in internet connectivity. Africa's average internet bandwidth is 21.12 megabits per second (Mbps), which is significantly lower than the worldwide average of 72.7 Mbps (Ndembi et al., 2025). Rural areas are most impacted by weak infrastructure (Mwogosi, 2025b). While urban settings are implementing AI health interventions in hospitals, rural healthcare providers are experiencing frustrations due to their unreliable connectivity, rendering AI health tools ineffective (Mwogosi, 2025b). Studies touch on how structural constraints in LMICs weaken data protection capacity and the effectiveness of AI health interventions. Standley et al. (2025) note that many African nations lack the capital necessary to effectively deploy AI. AI health interventions require a strong internet connection, expensive computers, and data centres. Currently, many AI health interventions assume conditions in developing nations are similar to developed nations (Mwogosi, 2025a). This assumption hinders their effectiveness, as there is less data on people in LMICs and technical capacity is lower, resulting in a decreased quality of the model. To overcome this challenge, developing low-bandwidth interventions could provide those working and living in rural regions with access to AI health interventions (Mwogosi, 2025b).

Exploitation and Underfunding in ICT Sectors

Pantserev (2022) explores the various AI interventions in Sub-Saharan Africa (SSA) and argues that AI can be beneficial for modernizing the healthcare sector. However, the authors state that the region is vulnerable to cyberattacks, and the information and Communication Technology (ICT) sectors are severely underdeveloped, and consequently, unable to protect data from cyberattacks (Ndembi et al., 2025; Pantserev, 2022). In 2017, Africa lost an estimated $3.5 billion due to cybercrime (Pantserev, 2022). Despite the losses, African companies are reluctant to increase their spending on cybersecurity; 90% of companies are severely underfunding their cybersecurity departments, spending less than $10,000 USD on average (Pantserev, 2022). Moreover, there is a risk that large AI corporations may exploit workers and pay low wages, while also not training them on proper data protection protocols, making health data vulnerable to leakage (Standley et al., 2025).

Regulatory Gaps & Lack of Education

In addition to structural barriers, there is the “regulatory vacuum” and lack of knowledge in developing nations, leaving patients’ health data vulnerable and consequently, fueling a sense of distrust toward AI interventions for both providers and patients (Mwogosi, 2025b, p. 4) Many researchers and clinicians are not willing to share critical health data that could track patterns, due to weak data protection regulation (Obiora et al., 2024). This is emphasized in rural populations, who are unsure of how the data they are providing is protected (Mwogosi, 2025b).

WHO (2024) outlines that a main challenge for AI integration is the lack of education on digital technologies. Moreover, there is little trust between clinicians and AI technology as diagnostic models do not break down their “thought” process, leading healthcare workers to question the outcome’s validity (Mwogosi, 2025b). In a qualitative study done by Mwogosi (2025b), interviewees revealed that healthcare workers received little guidance on how to use AI health tools, reducing their effectiveness. Healthcare workers stated that the most training they would receive is one session, and they received no updates (Mwogosi, 2025b). This issue impacted rural workers disproportionately, as many had little foundational knowledge of technology (Mwogosi, 2025b).

Policy Analysis and Application

General Data Protection Regulation (GDPR)

The EU’s GDPR is considered one of the most robust data protection frameworks worldwide (Mantelero, 2021). Its strength lies in the specificity of its terms. Recital 35 of the GDPR defines health data as any information that discloses one’s mental or physical health, in the past present or future (2018). This can include diagnoses, treatment, physiological conditions, genetic information, and medical history (GDPR, 2018).

The GDPR also created the European Data Protection Board (EDPB), which oversees the national Data Protection Authorities (DPAs) (GDPR, 2018). DPAs are independent national bodies that have full authority to investigate and issue fines to companies that are not complying with the GDPR (Mwogosi & Simba, 2025; GDPR, 2018). Article 83(5) of the GDPR states that fines for severe violations can be up to 20 million euros or four percent of the company’s total revenue worldwide (GDPR, 2018). For example, a hospital in Portugal was fined 400,000 euros for violating GDPR principles by its national regulator, the Comissão Nacional de Protecção de Dados (CNPD) (Makulilo et al., 2025). The CNPD found that personal health data was accessible to an unnecessary number of workers in the hospital, which went against the GDPR's data minimization principle and the patient's rights to integrity and confidentiality (Makulilo et al., 2025). DPAs illustrate regulatory oversight and issue fines that encourage companies to adhere to data protection standards.

Article 42 and Recital 85 of the GDPR (2018) outline that companies must notify their DPA within 72 hours of becoming aware of the breach and must communicate to data breach to the person whose data has been leaked. Article 5(c) of the GDPR discusses data minimization, which ensures that only the data necessary for the companies should be collected to limit the amount of data at risk of breach (2018). Lastly, Articles 32 and 89 touch on the responsibility for data collectors to ensure that their systems are being tested regularly to ensure their safety and personal data must be encrypted or pseudonymized to hide personal identifiers (GDPR, 2018).

Alongside the GDPR is the GDPR Awareness Initiative, which builds awareness for patients on what their data rights are, and gives healthcare providers best practices to guide their data collection and storage (Mwogosi & Simba, 2025)

Personal Data Protection Act (PDPA)

Compared to other countries in the African Union (AU), Tanzania's PDPA is lagging with specificity (Makulilo et al., 2025). While PDPA classifies health data as sensitive, it does not provide explicit definitions for personal health data or biometric data (Makulilo et al., 2025). This ambiguity creates room for interpretation in applying the PDPA regulations on how personal data may be processed. (Makulilo et al., 2025). There is a lack of awareness for both data subjects and healthcare providers. Many people are not aware of what their data rights are, and healthcare providers are unaware of how to collect and process data, leaving health data vulnerable to breaches (Mwogosi & Simba, 2025)

Additionally, the PDPC created by the PDPA is closely coupled with the government and does not operate independently, which limits its ability to enforce penalties for data misuse (Makulilo et al., 2025). Unlike the GDPR, where independent DPAs can issue substantial financial fines for non-compliance, there is no formalized framework for compliance monitoring, no detailed requirements for security protocols, and no nation-wide to prevent data leakage or unauthorized sharing (Mwogosi & Simba, 2025). Due to the limited guidance provided by the PDPA, healthcare providers are often unsure of how to properly comply with data protection, storage, and sharing (Goodman et al., 2023; Mwogosi & Simba, 2025).

The GDPR and PDPA overlap in their commitment to ensure that data remains localized within their countries and is not shared outside the nation unless it complies with specific regulations (Makulilo et al., 2025). Moreover, both state that entities controlling data must keep data confidential and integral, but the GDPR goes into more detail and adds enforcement mechanisms such as fines (Makulilo et al., 2025, GDPR, 2018)

Case Study: Pandemic Surveillance and AI Intervention

AI can be implemented for pandemic surveillance by enabling real-time monitoring and modelling disease transmission (Li et al., 2025). It can be incorporated into electronic health records (EHR) and analyze lab results, medication, diagnoses and unstructured data such as diagnostic imaging, clinic notes (Li et al., 2025). AI has the ability to detect infections early, identifying disease markers across medical imaging scans, analyze social media, track mobility patterns, and study data from wearable health devices (Li et al., 2025). Essentially, AI can be embedded across multiple platforms that generate health-related data.

In March 2025, the Tanzanian Minister of Health (MoH) announced the integration of AI into the DHIS2, the country's national health information management system (Mustafa et al., 2023; Summey, 2025). DHIS2 was adopted nationally in 2010 (Mustafa et al., 2023). Healthcare workers can submit information electronically or on paper, where it is later digitized (Mustafa et al., 2023). DHIS2 is linked to Tanzania's electronic disease surveillance system, allowing health facilities to report infectious disease data across the country (Mustafa et al., 2023). The MoH announced that AI would now support DHIS2 by analyzing event-based reports, text messages sent to DHIS2, and community-generated signals, centralizing all the data into one system (Summey, 2025).

When applying this AI health intervention to the PDPA framework reveals caveats that could put people's data at risk. Due to the PDPAs' lack of definitions, it is unclear what counts as "health data", and there are no explicit rules on accountability for misuse or data breaches. Since this DHIS2 is connected to the electronic disease surveillance system, a single cyberattack risks exposing large volumes of sensitive data. The AI tool also depends on text message alerts, which could make the system vulnerable to data poisoning(Summey, 2025b); therefore, manipulated or false reports could distort the outputs and lead to AI hallucinations or harmful misinformation.

Strengthening Data Protection in Tanzania

The Tanzanian case exemplifies why robust legal frameworks and technical safeguards are crucial for safeguarding data in AI-driven health interventions. Strengthening governance requires an inclusive development process, connecting academics, healthcare workers, software developers, government employers, data controllers, and community members to ensure context-appropriate rules and reduce public fear around collecting and sharing data (Goodman et al., 2023; Mwogosi, 2025b; Obiora et al., 2024).

To address the risks identified in Tanzania's AI-enabled surveillance system, the country would benefit from technical safeguards such as federated learning to reduce centralization, differential privacy to limit re-identification, and cryptographic measures to ensure data is being protected throughout the whole process (Khalid et al., 2023). On the legal side, the PDPA lacks strong enforcement mechanisms and clear accountability rules, which are necessary to ensure that these protections are implemented in practice.

Since AI itself cannot be sued, scholars such as Naidoo (2024) propose a balanced legal approach to nurture AI innovation while still holding those responsible accountable when there is a mistake. This includes the sandbox approach, which is a safe testing zone where companies can practice AI models without as many rules constraining them and dispute-resolution to determine responsibility if an AI system causes harm (Naidoo, 2024).

Technical Safeguards

Khalid et al. (2023) present multiple privacy-preserving machine learning (PPML) techniques that can protect sensitive health data in AI health interventions, while measuring their strengths and weaknesses. By embedding these safeguards into the PDPA, Tanzania could create clear legal requirements that compel AI health interventions to protect sensitive health data.

Federated Learning localizes data on the device rather than sending raw information to a central server; instead, only model updates are shared, allowing the AI system to improve without exposing sensitive data (Khalid et al., 2023). Differential privacy (DP) is employed by adding controlled “noise” to datasets, making it harder for unauthorized users to re-identify individuals, but still allowing the model to detect patterns (Khalid et al., 2023).

The authors also present several cryptographic approaches which secure data during computation. Secure multiparty computation (SMPC) allows multiple parties to jointly train on a model without seeing the other inputs (Khalid et al., 2023). Garbled circuits operate similarly but only involve two parties performing encrypted computations (Khalid et al., 2023). Lastly, secret sharing protects information by fragmenting data; as a result, if there is a data breach or partial leakage, no single fragment reveals identifiable information for the entire dataset (Khalid et al., 2023).

However, it is important to note that while the technical safeguards presented are innovative and hold to ability to protect health data in AI health interventions, LMICs often already experience resource constraints, and these systems would require sufficient technological and human capital to employ effectively (Panteli et al., 2025).

Limitations

This review faced multiple constraints that influenced the scope and representativeness of findings. First, a geographic imbalance was observed in the available literature, with a disproportionate overrepresentation of studies focused on South Africa in comparison to other African Nations. Second, locating relevant studies posed search term specificity challenges. Initial searches using broader terms, such as “health,” were found to be overbroad and needed refinement of search strings, leading to minor inconsistencies across search protocols. Furthermore, searches for specific terms such as “AI Hallucinators” yielded studies in the clinical and psychiatric fields rather than AI model errors. The results on the search for "misinformation" returned studies on the intersection of social media and misinformation instead of misinformation produced by AI health interventions.

Gaps and Areas of Future Research

The main gap identified in the literature is the limited research examining how AI health interventions can contribute to data misuse and how data can be protected post-breach. While studies discuss data misuse in general health systems, very few touch on how health data can be reidentified and incorporated back into AI systems, making it effectively impossible for individuals to regain control over their information once a leak occurs. Although many studies outlined the "challenges" linked to AI health interventions, there were rarely any case studies exemplifying how these breaches could happen. The lack of examples limits our ability to understand the specific mechanisms of how AI health interventions can fail in practice.

In the future, researchers should focus on technical safeguards needed for post-breach data protection, including whether data can be re-anonymized after re-identification or other measures that can be taken to protect an individual's data post-leak. This gap is significant since healthcare and governments are often coupled; if government-promoted AI health interventions experience data leaks, this can erode public trust in the government and healthcare systems.

Conclusion

In conclusion, this paper aimed to explore literature discussing the risks of data misuse in AI health interventions and understand what safeguards exist, or should exist, to prevent a privacy breach. AI health interventions create data integrity risks, perpetuate bias, and expose personal health data to re-identification risks. Additionally, the literature revealed structural constraints such as poor infrastructure, weak regulation, limited digital literacy, and underfunded cybersecurity. Although AI has the potential to help prevent pandemic outbreaks, Tanzania's regulatory frameworks need stronger compliance mechanisms to ensure that data controllers are take appropriate measures to protect sensitive health data.

AI Disclosure: Please note that AI was used in this paper to support outlining, conduct preliminary background research, and help explain terms according to the literature (e.g., blockchain, federated learning, and differential privacy)

References

Bandeira, A., Gonçalves, L. H., Holl, F., Shaibu, J. U., Gonçalves, M. L., Payinda, R., Paudel, S., Berionni, A., Wfpha, Y., Purnat, T. D., & Mackey, T. (2025). Viewpoint on the Intersection Among Health Information, Misinformation, and Generative AI Technologies. *JMIR Infodemiology*, *5*(1), e69474. https://doi.org/10.2196/69474

Chen, Y., & Esmaeilzadeh, P. (2024). Generative AI in Medical Practice: In-Depth Exploration of Privacy and Security Challenges. *Journal of Medical Internet Research*, *26*(1), e53008. https://doi.org/10.2196/53008

Denecke, K., Lopez-Campos, G., Rivera-Romero, O., & Gabarron, E. (2025). The Unexpected Harms of Artificial Intelligence in Healthcare: Reflections on Four Real-World Cases. In *Healthcare of the Future 2025* (pp. 55–60). IOS Press. https://doi.org/10.3233/SHTI250219

Goodman, K. W., Litewka, S. G., Malpani, R., Pujari, S., & Reis, A. A. (2023). Global health and big data: The WHO's artificial intelligence guidance. *South African Journal of Science*, *119*(5–6), 14725. https://doi.org/10.17159/sajs.2023/14725

Khalid, N., Qayyum, A., Bilal, M., Al-Fuqaha, A., & Qadir, J. (2023). Privacy-preserving artificial intelligence in healthcare: Techniques and applications. *Computers in Biology and Medicine*, *158*, 106848. https://doi.org/10.1016/j.compbiomed.2023.106848

Li, J.-H., Tseng, Y.-J., Chen, S.-H., & Chen, K.-F. (2025). Artificial Intelligence in Infection Surveillance: Data Integration, Applications and Future Directions. *Biomedical Journal*, 100929. https://doi.org/10.1016/j.bj.2025.100929

Makulilo, A., Mwamlangala, D., Ezekiel, R., Buchner, B., März, E., & Freye, M. (2025). Data privacy and security in E-health: African and European perspectives. *International Cybersecurity Law Review*, *6*(2), 195–206. https://doi.org/10.1365/s43439-025-00141-9

Mantelero, A. (2021). The future of data protection: Gold standard vs. global standard. *Computer Law & Security Review*, *40*, 105500. https://doi.org/10.1016/j.clsr.2020.105500

Mustafa, U., Kreppel, K. S., Brinkel, J., & Sauli, E. (2023). Digital Technologies to Enhance Infectious Disease Surveillance in Tanzania: A Scoping Review. *Healthcare*, *11*(4), 470. https://doi.org/10.3390/healthcare11040470

Mwogosi, A. (2025a). Ethical and privacy challenges of integrating generative AI into EHR systems in Tanzania: A scoping review with a policy perspective. *DIGITAL HEALTH*, *11*, 20552076251344385. https://doi.org/10.1177/20552076251344385

Mwogosi, A. (2025b). Leveraging AI to Enhance Healthcare Delivery in Tanzania: Innovations and Ethical Imperatives. *Sage Open*, *15*(3), 21582440251378162. https://doi.org/10.1177/21582440251378162

Mwogosi, A., & Simba, R. (2025). Digital policy and governance frameworks for EHR systems in Tanzania: A scoping review. *Digital Policy, Regulation and Governance*. https://doi.org/10.1108/DPRG-11-2024-0289

Naidoo, T. (2024). Overview of AI regulation in healthcare: A comparative study of the EU and South Africa. *South African Journal of Bioethics and Law*, e2294–e2294. https://doi.org/10.7196/SAJBL.2024.v17i3.2294

Ndembi, N., Rammer, B., Fokam, J., Dinodia, U., Tessema, S. K., Nsengimana, J. P., Mwangi, S., Adzogenu, E., Dongmo, L. T., Rees, B., O'Connor, B., Crowell, T. A., James, W., Colizzi, V., Ngongo, N., & Kaseya, J. (2025). Integrating artificial intelligence into African health systems and emergency response: Need for an ethical framework and guidelines. *Journal of Public Health in Africa*, *16*(1), 876. https://doi.org/10.4102/jphia.v16i1.876

Obiora, O. L., Shead, D. A., & Olivier, B. (2024). Data sharing considerations and practice among health researchers in Africa: A scoping review. *DIGITAL HEALTH*, *10*, 20552076241290955. https://doi.org/10.1177/20552076241290955

Panteli, D., Adib, K., Buttigieg, S., Goiana-da-Silva, F., Ladewig, K., Azzopardi-Muscat, N., Figueras, J., Novillo-Ortiz, D., & McKee, M. (2025). Artificial intelligence in public health: Promises, challenges, and an agenda for policy makers and public health institutions. *The Lancet Public Health*, *10*(5), e428–e432. https://doi.org/10.1016/S2468-2667(25)00036-2

Pantserev, K. A. (2022). Malicious Use of Artificial Intelligence in Sub-Saharan Africa: Challenges for Pan-African Cybersecurity. *Vestnik RUDN. International Relations*, *22*(2), 288–302. https://doi.org/10.22363/2313-0660-2022-22-2-288-302

Standley, C. J., Breugelmans, J. G., Chaudhari, A., Cherian, N., Chwalek, S., Deol, A., Dietrich, J., du Moulin, L., Otim, G., James, W., Kloth, S., Masmoudi, S., Ndembi, N., Ndlovu, N., Scarponi, D., Schnetzinger, F., Shapiro, M., & Hebbeler, A. (2025). Artificial intelligence for health security in Africa: Benefits, risks and opportunities. *Epidemics*, *53*, 100870. https://doi.org/10.1016/j.epidem.2025.100870

Sukums, F., Mzurikwao, D., Sabas, D., Chaula, R., Mbuke, J., Kabika, T., Kaswija, J., Ngowi, B., Noll, J., Winkler, A. S., & Andersson, S. W. (2023). The use of artificial intelligence-based innovations in the health sector in Tanzania: A scoping review. *Health Policy and Technology*, *12*(1), 100728. https://doi.org/10.1016/j.hlpt.2023.100728

Summey, E. (2025, March 31). AI-Driven Alert Triage with DHIS2 Transforms Disease Surveillance in Tanzania. *DHIS2*. https://dhis2.org/ai-driven-alert-triage-tanzania/

Townsend, B. A. (2025). Governance-by-Design as an Enabler of AI in Digital Health in Sub-Saharan Africa. *Law, Technology and Humans*. https://doi.org/10.5204/lthj.3975

Valle-Cruz, D., García-Contreras, R., & Gil-Garcia, J. R. (2024). Exploring the negative impacts of artificial intelligence in government: The dark side of intelligent algorithms and cognitive machines. *International Review of Administrative Sciences*, *90*(2), 353–368. https://doi.org/10.1177/00208523231187051

WHO. (2024). *Ethics and Governance of Artificial Intelligence for Health: Large Multi-Modal Models. WHO Guidance* (1st ed). World Health Organization. https://iris.who.int/server/api/core/bitstreams/e9e62c65-6045-481e-bd04-20e206bc5039/content

Appendix A.
Search Strategy Chart

Search Term #1				
“Artificial Intelligence” AND “Healthcare” AND “Weaponization”	Nov 20th	Google Scholar	2,620	5
		Biomed Central	1	0
		PubMed	0	0
		Scopus	0	0
		Science Direct	144	6
Database	Title	Type		
Google Scholar	Healthcare violence and the potential promises and harms of artificial intelligence	PRJ		
	Psychological Warfare in the Digital Age: Using Health Misinformation as a Cyber Weapon	Book Chapter		
	Technological advances and evolution of biowarfare: A threat to public health and security	PRJ		
	Regulating AI in nursing and healthcare: Ensuring safety, equity, and accessibility in the era of federal innovation policy			
	Exploring the negative impacts of artificial intelligence in government: the dark side of	PRJ		

Search Term #1		
	intelligent algorithms and cognitive machines	
Biomed Central	No Results	No Results
Pub Med	No Results	No Results
Science Direct	Artificial intelligence for health security in Africa: Benefits, risks and opportunities	PRJ
	Application of big data and artificial intelligence in epidemic surveillance and containment	PRJ
	Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions	PRJ
	Inalienable data: Ethical imaginaries of de-identified health data ownership	PRJ
	Privacy-preserving artificial intelligence in healthcare: Techniques and applications	PRJ
	Generative AI in Medical Practice: In-Depth Exploration of Privacy and Security Challenges	PRJ
Scopus	No Results	No Results

Search Term #2				
"“Artificial Intelligence” AND “Digital Health” AND “Africa” AND "Data Protection""	Nov 15th, 2025	Google Scholar	4830	21
		BMC	66	6
		Pub Med	3	2
		Scopus	3	3
		Science Direct	199	6
Database	Title	Type		
Google Scholar	Governance-by-Design as an Enabler of AI in Digital Health in Sub-Saharan Africa	PRJ		
	Strengthening population and public health data governance in the era of digital technology in Africa	PRJ		
	Data revolution, health status transformation and the role of artificial intelligence for health and pandemic preparedness in the African context	PRJ		
	Mapping the regulatory landscape of AI in healthcare in Africa	PRJ		
	Data privacy in healthcare: Global challenges and solutions	PRJ		
	Regulatory challenges of digital health: the case of mental health applications and personal data in South Africa	PRJ		

	Global health and big data: The WHO's artificial intelligence guidance	PRJ
	Legal mechanisms for digital healthcare transformation in Africa: state and perspective	PRJ
	Challenges and opportunities of artificial intelligence in African health space	PRJ
	Why are digital health policies crucial?	PRJ
	Overview of AI regulation in healthcare: A comparative study of the EU and South Africa	PRJ
	Integrating artificial intelligence into African health systems and emergency response: Need for an ethical framework and guidelines	PRJ
	Data sharing considerations and practice among health researchers in Africa: A scoping review	PRJ
	Ethical and privacy challenges of integrating generative AI into EHR systems in Tanzania: A scoping review with a policy perspective	PRJ
	Digital policy and governance frameworks for EHR systems in Tanzania: a scoping review	PRJ

	Empowering Africa: An in-depth exploration of the adoption of artificial intelligence across the continent	PRJ
	Tanzania's and Germany's digital health strategies and their consistency with the World Health Organization's global strategy on digital health 2020-2025 …	PRJ
	The role of digital health in pandemic preparedness and response: securing global health?	PRJ
	Cross-border data sharing for research in Africa: An analysis of the data protection and research ethics requirements in 12 jurisdictions	PRJ
	Operationalizing health data governance for AI innovation in low-resource government health systems: a practical implementation perspective from Zanzibar	PRJ
	Artificial intelligence in public health: promises, challenges, and an agenda for policy makers and public health institutions	PRJ
	Stopped after Page 15	
BMC	Data revolution, health status transformation and the role of artificial intelligence for health and pandemic preparedness in the African context	PRJ
	Ethical implications related to processing of personal data and artificial intelligence in	PRJ

	humanitarian crises: a scoping review	
	Epidemic intelligence in Europe: a user needs perspective to foster innovation in digital health surveillance	PRJ
	Artificial intelligence in healthcare: a scoping review of perceived threats to patient rights and safety	PRJ
	Artificial intelligent tools: evidence-mapping on the perceived positive effects on patient-care and confidentiality	PRJ
	Introduction and acceptability of the Surveillance Outbreak Response Management and Analysis System (SORMAS) during the COVID-19 pandemic in Côte d'Ivoire	PRJ
Pub Med	Data revolution, health status transformation and the role of artificial intelligence for health and pandemic preparedness in the African context	PRJ
	Mapping the regulatory landscape of AI in healthcare in Africa.	PRJ
Scopus	Mapping the regulatory landscape of AI in healthcare in Africa	PRJ

	Legal mechanisms for digital healthcare transformation in Africa: state and perspective	PRJ
	Data revolution, health status transformation and the role of artificial intelligence for health and pandemic preparedness in the African context	PRJ
Science Direct	Tanzania’s and Germany’s Digital Health Strategies and Their Consistency With the World Health Organization’s Global Strategy on Digital Health 2020-2025: Comparative Policy Analysis	PRJ
	Artificial intelligence and infectious disease diagnostics: state of the art and future perspectives	PRJ
	AI-driven innovations for enhancing mental health care in Tanzania: opportunities and challenges	PRJ
	A systematic analysis of failures in protecting personal health data: A scoping review	PRJ

	Viewpoint on the Intersection Among Health Information, Misinformation, and Generative AI Technologies	PRJ
	Are AI-based surveillance systems for healthcare-associated infections ready for clinical practice? A systematic review and meta-analysis	PRJ

Search Term #3				
“Artificial Intellgience” AND “Hallucinations” AND “Health”	Nov 19th, 2025	Google Scholar	18,800	8
		Biomed Central	0	0
		PubMed	0	0
		Scopus	0	0
		Science Direct	0	0
Database	Title	Type		
Google Scholar	Strategies for the Analysis and Elimination of Hallucinations in Artificial Intelligence Generated Medical Knowledge	PRJ		

	Reference hallucination score for medical artificial intelligence chatbots: development and usability study	PRJ
	False responses from artificial intelligence models are not hallucinations	Book Chapter
	Reducing Hallucinations and Trade-Offs in Responses in Generative AI Chatbots for Cancer Information: Development and Evaluation Study	PRJ
	Artificial intelligence in healthcare: ChatGPT and beyond	PRJ
	The clinicians' guide to large language models: A general perspective with a focus on hallucinations	PRJ
	Generative artificial intelligence and misinformation acceptance: An experimental test of the effect of forewarning about artificial intelligence hallucination	PRJ
	Use of artificial intelligence chatbots in interpretation of pathology reports	PRJ
Notes: Hallucinations kept bringing up schizophrenia		

Search Term #4

“Artificial Intelligence” and “Health Interventions” AND “Misinformation”	Nov 7th, 2025	Google Scholar	4,490	10
		Biomed Central	174	4
		PubMed	6	2
		Scopus	8	0
		Science Direct	359	10

Database	Title	Type
Google Scholar	AI Applications in Public Health: A Review of Epidemic Monitoring, Epidemiological Analysis, and Health Management	PRJ
	Harnessing artificial intelligence and digital technology for enhancing routine immunization among zero-dose children	PRJ
	Artificial Intelligence and Digital Technologies Against Health Misinformation: A Scoping Review of Public Health Responses	PRJ
	Online Interventions Addressing Health Misinformation: Scoping	PRJ
	Leveraging chatbots to combat health misinformation for older adults: Participatory design study	PRJ

	Assessing the accuracy of generative conversational artificial intelligence in debunking sleep health myths: mixed methods comparative study with expert	PRJ
	The application of Generative AI for Personalized Health Messaging to Promote Public Health Awareness in Nigeria	IDK
	The Future of Public Health: Integrating Artificial Intelligence in Disease Surveillance and Prevention	IDK
	I trust you, but let me talk to AI: The role of the chat agents, empathy, and health issues in misinformation guidance	PRJ
	Early detection and control of the next epidemic wave using health communications: development of an artificial intelligence-based tool and its validation on …	PRJ
Biomed Central	Harnessing the power of artificial intelligence for disease-surveillance purposes	PRJ
	Artificial intelligence in healthcare: a scoping review of perceived threats to patient rights and safety	PRJ
	Psychiatrists' and trainees' knowledge, perception, and readiness for integration of	PRJ

	artificial intelligence in mental health care in Nigeria	
	Ethical implications related to processing of personal data and artificial intelligence in humanitarian crises: a scoping review	PRJ
Pub Med	Era of Generalist Conversational Artificial Intelligence to Support Public Health Communications.	PRJ
	The Unexpected Harms of Artificial Intelligence in Healthcare: Reflections on Four Real-World Cases.	PRJ
Science Direct	Era of Generalist Conversational Artificial Intelligence to Support Public Health Communications	PRJ
	Artificial Intelligence in Infection Surveillance: Data Integration, Applications and Future Directions	PRJ
	Artificial intelligence and infectious diseases: Scope and perspectives	PRJ
	Viewpoint on the Intersection Among Health Information, Misinformation, and Generative AI Technologies	PRJ
	Using artificial intelligence and predictive modelling to enable learning healthcare systems (LHS) for pandemic preparedness	PRJ
	Chapter 18: Big data and artificial intelligence for pandemic preparedness	Book Chapter

	Chapter 22: Artificial intelligence and public health: challenges and opportunities	Book Chapter
	Artificial intelligence for COVID-19: battling the pandemic with computational intelligence	PRJ
	The medical and societal impact of big data analytics and artificial intelligence applications in combating pandemics: A review focused on Covid-19	PRJ
Scopus	0	

<table>
<tr><th colspan="5">Search Term #5</th></tr>
<tr><td rowspan="5">“Artificial Intelligence” AND “ Health” “Tanzania”</td><td rowspan="5">Nov 15th, 2025</td><td>Google Scholar</td><td>2740</td><td>8</td></tr>
<tr><td>Biomed Central</td><td>83</td><td>1</td></tr>
<tr><td>PubMed</td><td>19</td><td>3</td></tr>
<tr><td>Scopus</td><td>10</td><td>2</td></tr>
<tr><td>Science Direct</td><td>153</td><td>4</td></tr>
<tr><td>Database</td><td>Title</td><td colspan="3">Type</td></tr>
<tr><td rowspan="2">Google Scholar</td><td>The use of artificial intelligence-based innovations in the health sector in Tanzania: A scoping review</td><td colspan="3">PRJ</td></tr>
<tr><td>Tanzania's and Germany's digital health strategies and their consistency with the World</td><td colspan="3">PRJ</td></tr>
</table>

	Health Organization's global strategy on digital health 2020-2025 …	
	Leveraging AI to Enhance Healthcare Delivery in Tanzania: Innovations and Ethical Imperatives	PRJ
	Ethical and privacy challenges of integrating generative AI into EHR systems in Tanzania: A scoping review with a policy perspective	PRJ
	AI-driven innovations for enhancing mental health care in Tanzania: opportunities and challenges	PRJ
	Impact and challenges of artificial intelligence integration in the African health sector: a review	PRJ
	Digital policy and governance frameworks for EHR systems in Tanzania: a scoping review	PRJ
	Artificial Intelligence in African Healthcare: Catalyzing Innovation While Confronting Structural Challenges	PRJ
Biomed Central	Data revolution, health status transformation and the role of artificial intelligence for health and pandemic preparedness in the African context	PRJ

Pub Med	Ethical and privacy challenges of integrating generative AI into EHR systems in Tanzania: A scoping review with a policy perspective.	PRJ
	Tanzania's and Germany's Digital Health Strategies and Their Consistency With the World Health Organization's Global Strategy on Digital Health 2020-2025: Comparative Policy Analysis.	PRJ
	Mapping the regulatory landscape of AI in healthcare in Africa.	PRJ
Scopus	Tanzania’s and Germany’s Digital Health Strategies and Their Consistency With the World Health Organization’s Global Strategy on Digital Health 2020-2025: Comparative Policy Analysis	PRJ
	Mapping the regulatory landscape of AI in healthcare in Africa	PRJ
Science Direct	Tanzania’s and Germany’s Digital Health Strategies and Their Consistency With the World Health Organization’s Global Strategy on Digital Health 2020-2025: Comparative Policy Analysis	PRJ
	The use of artificial intelligence-based innovations in the health sector in Tanzania: A scoping review	PRJ
	Evaluating predictive artificial intelligence approaches used in mobile health platforms to forecast mental health symptoms among youth: a systematic review	PRJ

	Exploring the impact of generative AI tools on healthcare delivery in Tanzania	PRJ

Search Term #6

"Tanzania" AND "Data Protection" AND "Artificial Intelligence" AND "Health Data"	Nov 18th, 2025	Google Scholar	542	
		Biomed Central	8	1
		PubMed	1	1
		Scopus	1	1
		Science Direct	23	
Database	Title	Type		
Google Scholar	Protection of Personal Data in E-Health: A Comparative Perspective Between Tanzania and Germany.	PRJ		
	Strengthening protection of personal data in the health sector: a comparative analysis of the Tanzanian and German eHealth system	PRJ		
	Data protection law: Lessons from Tanzania for South Africa?	PRJ		
	Digital policy and governance frameworks for EHR systems in Tanzania: a scoping review			
	[PDF] uct.ac.za Privacy and data protection in eHealth in Africa-an assessment of the regulatory frameworks that govern privacy and data	PRJ		

	protection in the effective implementation of …	
	Ethical and privacy challenges of integrating generative AI into EHR systems in Tanzania: A scoping review with a policy perspective	PRJ
	Blockchain technology in sub-saharan africa: Where does it fit in healthcare systems: A case of tanzania	PRJ
	The regulation of health data sharing in Africa: a comparative study	PRJ
	Mapping the regulatory landscape of AI in healthcare in Africa	PRJ
	'Potato potahto'? Disentangling de-identification, anonymisation, and pseudonymisation for health research in Africa	PRJ
	Influence of security monitoring practices on security of electronic health records in Tanzanian public hospitals.	PRJ
	Leveraging AI to Enhance Healthcare Delivery in Tanzania: Innovations and Ethical Imperatives	PRJ

	Data privacy and security in E-health: African and European perspectives: The example of post data protection legislation in Tanzania	PRJ
Biomed	Data revolution, health status transformation and the role of artificial intelligence for health and pandemic preparedness in the African context	PRJ
PubMed	Mapping the regulatory landscape of AI in healthcare in Africa	PRJ
Scopus	Mapping the regulatory landscape of AI in healthcare in Africa	PRJ
Science Direct	Artificial intelligence for health security in Africa: Benefits, risks and opportunities	PRJ
	AI-driven innovations for enhancing mental health care in Tanzania: opportunities and challenges	PRJ
	Tanzania's and Germany's Digital Health Strategies and Their Consistency With the World Health Organization's Global Strategy on Digital Health 2020-2025: Comparative Policy Analysis	PRJ
	Patients' Perspectives on the Data Confidentiality, Privacy, and Security of mHealth Apps: Systematic Review	PRJ

Search Term #7				
'“Artificial Intelligence” AND "Data Leak" AND "Health" AND “Africa”	Nov 21th, 2025	Google Scholar	478	4
		Biomed Central	1	1
		PubMed	0	0
		Scopus	0	0
		Science Direct	58	0
Database	Title	Type		
Google Scholar	Malicious use of artificial intelligence in Sub-Saharan Africa: Challenges for Pan-African cybersecurity	PRJ		
	Privacy Perceptions on Personal Data and Data Breaches in South Africa	PRJ		
	Understanding data breach from a global perspective: Incident visualization and data protection law review	PRJ		
	Technical and regulatory challenges of digital health implementation in developing countries	PRJ		
BMC	Artificial intelligent tools: evidence-mapping on the perceived positive effects on patient-care and confidentiality	PRJ		
PubMed	No Results			
Science Direct	No Results			

Search Term #8				
"Artificial Intelligence" AND "Tanzania" AND "Pandemic Preparedness"	Nov 21st	Google Scholar	428	6
		Biomed	11	1
		Pubmed	1	1
		Scopus	0	0
		Science Direct	28	2
Databse	Title	Type		
Google Scholar	Data revolution, health status transformation and the role of artificial intelligence for health and pandemic preparedness in the African context	PRJ		
	Examining the Implementation of Digital Health to Strengthen the COVID-19 Pandemic Response and Recovery and Scale up Equitable Vaccine Access in African Countries	PRJ		
	Ethical Implications of the Utilization of Artificial Intelligence (AI) in Vaccine Distribution Planning and Scheduling During Pandemic in Low-Middle-Income-Countries …	PRJ		
	Artificial Intelligence for Health Security in Africa: Benefits, Risks and Opportunities	PRJ		
	Big data analytics for integrated infectious disease surveillance in Sub-Saharan Africa	PRJ		
	Feasibility of a Mobile Application for Self and Assisted Reporting of Coronavirus Disease 2019 Self-Testing Results in Tanzania: A Pilot Study	PRJ		
Biomed	Data revolution, health status transformation and the role of artificial intelligence for health	PRJ		

	and pandemic preparedness in the African context	
Pubmed	Feasibility of a Mobile Application for Self and Assisted Reporting of Coronavirus Disease 2019 Self-Testing Results in Tanzania: A Pilot Study	PRJ
Scopus	No Results	PRJ
Science Direct	Artificial intelligence for health security in Africa: Benefits, risks and opportunities	PRJ
	Applications of Artificial Intelligence in the Control of Infectious Diseases in the Post-COVID Era: Scoping Review	PRJ