Governing Cross-Border Health-Data Transfers in AI-Guided Diagnostics: Effectiveness of Regional/International Frameworks for LMIC Data Sovereignty and Individual Protection

Nazanin Nasiri

Student Number: 101047744

Word count: 5527

Course Code: INAF5706

ABSTRACT

Artificial intelligence (AI) diagnostic and predictive tools increasingly depend on cross-border health-data transfers, raising questions regarding data sovereignty and individual protection in low- and middle-income countries (LMICs). This review asks: 1. How do existing global, regional and national frameworks govern cross-border health-data transfers for AI-guided tools? 2. How effective are these arrangements in LMIC practice? 3. What gaps remain for data sovereignty and individual rights? A structured search of Scopus, PubMed and Google Scholar (2020-2025) identified 28 peer-reviewed, preprint and grey-literature sources on AI diagnostics, health-data governance and LMIC data-transfers, screened using documented inclusion/exclusion criteria. The literature shows that cross-border AI health-data transfers are governed by global norms (GDPR, WHO), regional frameworks and national data-protection laws, accompanied by emerging "governance-by-design" framework, however, these tend to be fragmented, rarely AI-specific and unevenly interpreted. Implementation is limited by weak infrastructure, regulatory and ethical capacity and legal uncertainty, leaving gaps between formal protections and practice. Sovereignty and individual-rights risks persist where donor and vendor controlled infrastructures shape data flows, consent process is minimal, and accountability mechanisms are weak. Policy responses should prioritise AI-specific guidance under existing laws, cooperative oversight mechanisms and funding in privacy-preserving, locally controlled data architectures.

1. INTRODUCTION

1.1 AI Diagnostics and the Globalization of Health Data

AI-guided diagnostic and predictive health tools are increasingly becoming embedded in healthcare delivery worldwide. These systems often rely on large volumes of patient data and cloud-based algorithms which can send health information across national borders for storage or processing (Khalid et al., 2023; Seddon & Currie, 2013). For instance, diagnostic images or records collected in a low-resource hospital may be uploaded to vendor-hosted cloud platforms or out-of-country servers for AI model training and analysis. Such transfers can enable remote AI diagnostics and generate large health datasets that could improve care if used appropriately (Xia et al., 2024). However, this globalization of health data also exposes fundamental governance challenges as cross-border data transfers can exceed the effective scope of any single country's regulatory framework.

1.2 Data Sovereignty and Fragmented Cross-Border Governance

A core issue is data sovereignty which is the principle that nations exercise authority over data generated within their borders. Governments, including those in low- and middle-income countries (LMICs), are concerned that when their citizens' health data are stored/processed abroad, they may fall under foreign legal control, creating risks of access or exploitation and weakening national oversight (Sekalala & Chatikobo, 2024). At the same time, allowing health data to move freely across borders is regarded as vital for innovation and knowledge exchange, especially to use AI where domestic capacity is limited. However, global data governance is fragmented where regional and national frameworks take very different approaches to privacy, data flows, and security. Xia et al. (2024) argue that inconsistent cross-border data policies can negatively impact international medical research and telemedicine and create barriers for healthcare providers sharing patient information across regions. Together, these raise concerns that global health-data exchange may come at the expense of LMICs' sovereignty and oversight.

1.3 Individual-Level Protection in Cross-Border AI Data Flows

As equally important is the implication for individual-level protection of patients' data when health information is transferred to foreign systems. Once data leave the clinic and enter transnational cloud or vendor environments, they are often governed by a fragmented set of privacy laws with limited transparency and enforceability across borders; therefore, if data are mishandled/breached while stored internationally, cross-border jurisdictional complexities can make accountability and redress extremely difficult. Further, in many LMICs, individuals have limited awareness of how their health data are used in research or AI development beyond the original diagnostic purpose and may lack options to refuse or request deletion of their information (Davis et al., 2023). Studies have documented cases where AI vendors reused clinical data to train algorithms without obtaining new informed consent or providing notice to the individuals involved (Powles & Hodson, 2017). These scenarios jeopardize rights to privacy, information, and meaningful consent.

1.4 Structural Vulnerabilities and "Health Data Colonialism" in LMICs

Such concerns are particularly amplified in LMICs which often face structural vulnerabilities in the governance of digital health data. Many LMIC health systems struggle with limited digital infrastructure, including unstable electricity, inadequate internet bandwidth and a shortage of local AI and regulatory expertise, forcing them to rely on foreign cloud services and external companies to develop and manage AI diagnostic systems (Marey et al., 2025). Weak legal frameworks for data protection and AI oversight

can then be exploited by foreign actors. Ferryman (2021) describes this as a form of "health data colonialism" where institutions from high-income countries collect or host LMIC patient data to build AI algorithms under looser regulatory environments. In these scenarios, LMIC populations provide data that help create AI products, while the economic and clinical benefits accrue to companies and health systems in the Global North. External partnerships can therefore advance innovation while simultaneously weakening national interests or patient welfare. Ultimately, these issues define the central problem of this review regarding how cross-border health-data transfers in AI-guided diagnostic and predictive health tools can be governed so that LMICs can benefit from innovation without sacrificing data sovereignty or individual protection.

1.5 Scope, Research Questions, and Thesis Statement

This review focuses on AI-guided diagnostic and predictive health tools, and cross-border health-data transfers these systems trigger. It assesses regional and international frameworks that shape how LMIC health system actors and supervisory bodies govern these data-transfers. This review does not evaluate algorithmic accuracy, non-health AI use cases, or domestic implementations that do not involve cross-border transfers except where they discuss rights/governance issues. Within a broader scope, this paper deepens themes of safeguards, surveillance risk, individual rights and the digital divide by analyzing the cross-border data-governance layer that shapes each. It complements teammates' work on marginalized communities, weaponization of data in AI health systems, individual-level safeguarding and enforcement by identifying where regional and international frameworks enable or weaken protection in LMIC implementations and by highlighting system-level tools that national teams and Grand Challenges Canada (GCC) can use. Guided by this problem and scope, this paper addresses the following research questions:

1. How do existing regional and international data-protection and related digital-governance frameworks govern cross-border health-data transfers in AI-guided diagnostic and predictive health tools?
2. How effective are those frameworks and their enforcement mechanisms in protecting data in AI applications used in low- and middle-income countries?
3. What gaps remain for data sovereignty and individual protection?

In response to these questions, this paper argues that although regional and international frameworks articulate principles for cross-border health-data transfers and data-subject rights, their effectiveness for AI-guided diagnostics and predictive tools in LMICs is only partial because 1. legal frameworks for cross-border transfers are fragmented, often not AI-specific, and generate uncertainty about how health

data may be shared and reused, 2. implementation and enforcement capacity especially in LMIC supervisory bodies and health systems remains limited so protections that exist on paper frequently do not translate into practice, and 3. governance of cross-border health-data transfers often defaults to private contracts and infrastructures controlled by external vendors and cloud providers while technical and organizational safeguards are unevenly adopted in LMICs.

2. METHODS

2.1 Sources

Scopus was selected as the first database as its coverage of interdisciplinary health policy journals made it appropriate for capturing comparative data-governance and regulatory analyses. PubMed was used to identify health-specific articles on AI diagnostics, digital health-data use, and privacy/ethics in clinical implementations. Lastly, Google Scholar was used to capture preprints not yet published in Scopus/PubMed, policy and legal analyses, and reports and guidance from international organizations given the novelty of cross-border AI health-data governance and the likelihood that relevant work appears as preprints, conference proceedings or institutional reports.

2.2 Strategy

Searches were conducted between 7-9 November 2025. For each database, specific Boolean strings combined terms for AI, diagnostics/health data, cross-border transfers, governance/framework, and LMIC settings. Full strings, dates, hit counts, and included articles are reported in Appendix A. For Scopus, the 2 strings used the TITLE-ABS-KEY in the advanced search to ensure that the selected terms appeared in the title, abstract, or keywords. For PubMed, the Advanced Search Builder was used to run two strings. The initial string output very few results in both databases; therefore, the second string was broadened to capture a wider list of sources. For Google scholar, three strings were used to capture pre-print, peer-reviewed and grey literature and the results were ordered by relevance.

2.3 Screening & eligibility

Screening occurred using pre-specified inclusion and exclusion criteria summarized in Appendix B. Across databases, searches were limited to English language publications from 2020 to 2025, reflecting the rapid expansion of AI diagnostics and recent data-protection reforms. For Google Scholar, screening proceeded page by page and the search for a given string was stopped once a full page of results yielded no additional potentially relevant title/abstracts. 202 sources were screened by title to assess relevance to

AI-guided diagnostic or predictive health tools (or closely related digital health/health-data uses), and governance of health or health personal data (regulation, data protection, cross-border transfer, or ethics) with explicit relevance for LMICs or South-North data-transfers. Of those, 75 were reviewed by abstract and further 39 were retrieved for full text review and assessed against the inclusion/exclusion criteria as mentioned in Appendix B. In total, 28 sources met the inclusion criteria and were retained for analysis, comprising 20 peer reviewed articles, 2 preprints, and 6 grey literature reports or guidance documents (see Appendix C).

2.4 Data extraction & Synthesis

For each included source, key characteristics were extracted into a spreadsheet (Appendix D demonstrates two examples of the extraction), including region, type of AI use (diagnostics, predictive risk modelling, public-health surveillance, broader digital health), governing legal or policy frameworks mentioned; key findings and study design. The results were then synthesized thematically in line with the research questions.

3.0 LITERATURE REVIEW

3.1 Regulatory frameworks for cross-border health-data flows

Across the current literature, the governance of cross-border health-data for AI-guided tools is shaped by a combination of global, regional, national and technical frameworks rather than a single AI-specific treaty. At the global level, frameworks such as the GDPR and WHO's Ethics and Governance of AI for Health guidance set reference standards for data protection, cross-border transfers and individual rights (Bernier et al., 2024; WHO, 2021). Under the GDPR, health data may leave the European Economic Area only when conditions of adequacy decision, standard contractual clauses or limited derogations are met; therefore, these extraterritorial transfer rules transfer EU standards to international collaborations, requiring LMIC partners to meet EU-level safeguards even when their own laws are weaker or differently structured (Bernier et al., 2024; Nwachukwu, 2025). WHO's guidance and a LMIC-focused study similarly emphasize legality, purpose limitation, transparency, security and accountability as prerequisites for AI in health, and calls for an oversight of private platforms and public private partnerships involvement in cross-border health data processing (WHO, 2021; Junaid et al., 2025).

Regionally and nationally, African and other LMICs are moving quickly to implement general data-protection laws that classify health data as sensitive and require higher safeguards for processing and export. Munung et al. (2024) map 37 African data-protection frameworks and show that most recognize

core rights (access, rectification, erasure, compensation) and require either data-subject consent or adequacy in recipient countries for cross-border transfers in the context of health-research collaborations. Nienaber McKay et al. (2024) similarly discuss how Ghana, Kenya, Nigeria, South Africa and Uganda regulate health-data sharing, including consent requirements, data-sharing agreements and conditions for exporting data. However, both studies highlight wide variation in definitions, exceptions and enforcement powers, creating fragmentation in cross-border data transfer for South-North collaborations. Townsend et al. (2023) further suggest that no African country in their 12 state sample has a dedicated AI framework given AI in health is governed indirectly through data-protection laws, e-health strategies, and consumer-protection laws. Similar patterns appear in other regions as Wang et al. (2025) indicate that South Asian frameworks for telemedicine and AI-enabled early cancer detection rely on general digital-health and data-sharing policies rather than AI-specific legislation.

A number of country specific studies examine how these frameworks apply to AI-guided tools. In Ghana, the Data Protection Act 2012 and sectoral health laws provide a legal basis for regulating AI-based research and development; however, these were developed prior to modernization of AI and therefore contain gaps in algorithmic transparency, liability and export of sensitive health data (Mensah, Protecting Sensitive Health Data; Ethics and Privacy in AI Predictive Health). Similar concerns emerge in Donnelly's (2022) analysis of South Africa, which argues that existing medical device and telemedicine frameworks are poorly suited to adaptive AI systems and decision-support tools, and therefore require reform, particularly with regards to oversight of software as a medical device, informed-consent standards, allocation of liability, and product-liability obligations for developers and manufacturers. In Zanzibar, Li et al. (2024) use a case study of the government health-system to demonstrate how high level health-data governance principles for AI innovation can be operationalized in practice, developing guidelines for informed consent, data-access management and information security which includes standardized procedures for access control, data classification, de-identification and sharing with external researchers in a low-resource settings.

Beyond law, several authors highlight how system architectures and institutional data governance frameworks effectively act as regulatory mechanisms for cross-border AI. Hallock et al. (2021) and Arefin and Zannat (2025) suggest that federated health-data networks, where data stay local and algorithms travel to the data, combined with privacy preserving tools such as federated learning (AI model trained locally), blockchain auditing (tamper-resistant logging of data access) and AI-driven threat detection as ways to enable multi-country model training while keeping identifiable data in local nodes or controlled secure environments, therefore reducing the need for cross-border transfers and easing compliance with GDPR style rules. Townsend (2025) labels this approach as "governance-by-design"

which integrates legal and ethical principles/rules directly into health-system architectures, standards and workflows to address data integrity, provenance, interoperability and accountability challenges in sub-Saharan Africa. Kaushik et al. (2025) and Li et al. (2024) both show how data governance frameworks covering informed-consent processes, data-access management and security guidelines condition whether health systems can share and reuse clinical data for AI while remaining compliant with privacy and data-protection requirements. ECDPM's report on AI diagnostics in Africa also calls for EU-Africa partnerships to support health-data governance and sharing frameworks, strengthen certification capacity and data-centre infrastructure as part of scaling AI diagnostics (Apiko & Musoni, 2025). Finally, Towett et al. (2024) multi-disease digital health passport illustrates how pan-African digital platforms for cross-border health status verification would depend on continent wide agreements on data security standards, interoperability and privacy rights safeguards, in order to enhance surveillance and access to care without becoming infrastructures for unchecked data reuse or monitoring.

Taken together, these studies show that cross-border health-data flows for AI diagnostics are already governed, but through a fragmented patchwork of global norms, regional frameworks, national data-protection laws and technical architectures rather than a single law. Strong frameworks (GDPR) effectively set conditions for many international collaborations, while LMICs' general data-protection laws and emerging tools (federated networks/digital health passports) are increasingly used as part of the regulation. Analytically, this suggests that the core problem for RQ1 is not a complete absence of rules, but misalignment and gaps between legal layers and technical arrangements where governance depends heavily on how institutions and vendors interpret and combine together these frameworks in practice. AI-guided diagnostic and predictive tools therefore rarely fit within a dedicated cross-border framework, creating uncertainty about how consistently health-data are protected.

3.2 Effectiveness and implementation barriers in LMIC contexts

Across the selected studies, there is broad agreement that formal/on-paper protections often fail in practice in LMIC health-systems due to deficits in infrastructures, institutional capacity gaps and policy to practice inconsistencies. Sources that focus on AI in the Global South consistently highlight weak digital infrastructure, fragmented health information systems, and limited interoperability as key barriers to effective AI deployment and data governance enforcement (Hussain et al., 2025; Oladipo et al., 2024; Ndemo, 2025; Andigema et al., 2025). Kaushik et al.'s (2025) systematic review of LMIC data sharing for AI tools, complemented by a case study from Thailand, identifies unreliable connectivity, lack of equipment, inconsistent data standards and cybersecurity concerns as major technical barriers to data sharing. Similar challenges appear in Li et al.'s (2024) Zanzibar case, where routine health-data are poor

quality and capacity constraints make it difficult to implement data access and security guidelines in practice, limiting the impact of governance rules on access, security and consent. Wang et al. (2025) show similar patterns in South Asia's telemedicine and AI cancer-screening reforms with India's more advanced digital-health infrastructure and centralized governance enabling pilots and policy alignment, whereas Pakistan, Bangladesh and Nepal struggled with infrastructure gaps and fragmented systems.

Even where legal/institutional frameworks exist, regulatory and ethics bodies often lack AI literacy and resources to apply them. Olawade et al.'s (2026) qualitative study of Nigerian research ethics committees reveals that members are aware of AI's potential risks but feel unequipped to review AI projects as they lack training on algorithmic systems, have no AI-specific national guidance, and have significant concerns regarding data privacy, consent and sharing patient information with third parties. Similar capacity gaps at national level appear in analyses of African data-protection authorities and health regulators, which often face limited resources, fragmented legal frameworks, and weak enforcement capacity, making it difficult for them to issue clear guidance or systematically audit data uses (Prinsloo & Kaliisa, 2022; Munung et al., 2024; Nienaber McKay et al., 2024; Townsend et al., 2023). Junaid et al.'s (2025) systematic review on developing countries found that across 22 studies, concerns about data privacy, justice, cyber-security and transparency are repeatedly raised, yet many settings report weak or absent regulatory frameworks, limited cyber-security infrastructure and few policies to operationalize patients' rights and accountability. In fact, case studies of particular AI applications in clinical settings reinforces these findings. Della Ripa et al. (2025) document health worker perspectives on AI-enabled obstetric point-of-care ultrasound in LMICs, describing ongoing struggles with device maintenance, electricity, and staff training, which constrain tool performance and oversight. ECDPM's analysis of AI diagnostics in Africa similarly emphasizes that under-investment in hospital IT integration, cybersecurity and evaluation capacity limits safe implementation and the ability to certify tools or audit vendors. In Zanzibar, Li et al. (2024) show how putting data governance policies into measure (data-access management procedures and information-security guidelines) required substantial external technical support, an 18-month multi-stakeholder process and ongoing training, highlighting that implementing such frameworks in LMIC government health-systems is a major capacity-building effort rather than a one-time legal reform.

Lastly, several legal and policy analyses argue that regulatory fragmentation and legal uncertainty weaken effectiveness even where laws exist. Munung et al. (2024) and Nienaber McKay et al. (2024) show that inconsistencies in African rules on secondary use and cross-border export of health data create legal uncertainty and fear of sanctions for researchers, which can discourage data sharing and collaboration. Bernier et al. (2024) similarly argue that the stringent and complex GDPR requirements for international

data transfers place a heavy compliance burden on transnational data commons, sometimes inhibiting or delaying EU and non-EU (including LMIC) collaborations. Donnelly's (2022) South African analysis, Adebayo et al.'s (2025) Africa-EU comparison of AI for public-health surveillance, and Mensah's Ghana papers all suggest that many AI health applications in Africa are currently operating in a regulatory grey zone where they are put into older telemedicine, device and data-protection frameworks that were not designed for adaptive AI systems, and most countries still lack clear AI-specific health legislation; consequently, leaving uncertainty about how to allocate responsibilities for safety, liability and how to govern cross-border relationships with foreign AI and cloud vendors.

Overall, the evidence suggests that existing frameworks are only partially effective in LMIC practice. Technical/organizational weaknesses limit regulatory and ethical capacity, and legal fragmentation create a persistent implementation gap with principles of data protection and rights exist on paper but are not reliably applied in AI implementations. Analytically, these studies indicate that effectiveness depends less on the presence of high level norms and more on basic capacities such as connectivity, data quality, trained oversight bodies and clear rules for cross-border vendors, precisely where many LMICs are under-resourced. For RQ2, this implies that regional and international frameworks are necessary but not sufficient for protecting health data in AI-guided tools unless they are combined with investment in infrastructure, institutions and enforcement.

3.3 Gaps in data sovereignty and individual protection

The third theme from the sources obtained concerns what remains missing including who ultimately controls LMIC health data in AI systems, and how well individuals' rights are protected once their information enters transnational infrastructures. In fact, many authors worry that current frameworks risk reinforcing "data colonialism", where LMIC populations supply data for AI innovation without commensurate control, benefit or protection (Ndemo, 2025; Andigema et al., 2025; Apiko & Musoni, 2025; Hussain et al., 2025; Oladipo et al., 2024). These studies demonstrate how AI models are often trained on high income countries' datasets and then implemented in African or South-Asian settings or how local clinical data are exported to foreign cloud providers for model development and commercialization, with limited oversight from LMIC governments. Mensah's articles on Digital Sovereignty in the Age of AI and Protecting Sensitive Health Data frames the poorly regulated cross-border transfers of Ghanaian health data as threats to national data sovereignty, calling for structured data-access protocols, localization where appropriate, and regional cooperation to ensure that they can participate in global AI while retaining control over their own health data. Legal mapping studies highlight similar sovereignty concerns as Munung et al. (2024) and Nienaber & McKay (2024) show that

although many African countries now have data protection and data export provisions, rules for sharing health data across borders are incomplete and inconsistent with some jurisdictions lacking any explicit cross-border transfer clauses, while others offering minimal guidance on safeguards or secondary use. This regulatory uncertainty/gap is further complicated by the fact that the infrastructures and standards underlying many AI and data-sharing initiatives are significantly shaped by donors, multinational vendors or foreign research partnerships rather than by LMIC regulators themselves (Apiko & Musoni, 2025; Adebayo et al., 2025; Bernier et al., 2024). WHO (2021) similarly warns that AI health systems could concentrate power in larger technology companies, potentially compromising the autonomy of LMICs' patients and governments.

At the individual level, the sources highlight gaps in informed consent, privacy, security and remedy/recourse. Articles focusing on LMICs show that patients and clinicians often lack clarity as to when their data will be reused for AI or shared with external partners; several describe consent processes that they rely on are complex, legalistic forms do not explain secondary uses, or are missing altogether (Kaushik et al., 2025; Li et al., 2024; Olawade et al., 2023). Junaid et al.'s (2025) review finds data privacy and justice to be the most frequently raised ethical issues in developing-country AI healthcare, with recurrent concerns about data security, algorithmic bias, and cybersecurity, highlighting concerns regarding insufficiently accountable AI systems. Nwachukwu (2025) and Adepoju & Adepoju (2025) explain how AI analytics, data linkage and model-inversion attacks can re-identify individuals from anonymized datasets, challenging traditional de-identification approaches. WHO (2021), Arefin & Zannat (2025), and Hallock et al. (2021) all argue that strong security, minimization and privacy preserving architectures (federated learning, secure processing environments, tamper-evident ledgers) are essential components of individual protection in AI health research, but mirroring with Theme 2, their deployment in LMIC health systems is limited.

Further, accountability and liability are another major identified gap. Donnelly's (2022) analysis of South African law highlights difficulties applying traditional negligence doctrines to AI-driven decisions, leading to uncertainty regarding who would be responsible when an AI diagnostic tool contributes to patient harm. Moreover, Olawade et al. (2026) report that Nigerian ethics committee members are unsure which government bodies currently have clear responsibility for overseeing AI in healthcare and emphasize the need for a coordinated, multi-stakeholder regulatory approach. Junaid et al. (2025) and WHO (2021) highlight that weak accountability around AI in healthcare leave patients with limited options for compensation and oversight. Townsend (2025) and Towett et al. (2024) extend this concern to broader infrastructures arguing that digital health passports or AI-enabled surveillance systems could

easily become tools of disproportionate monitoring or exclusion if they are not subject to democratic control, independent oversight and strong rights protections.

Taken together, the literature suggests that gaps in data sovereignty and individual protection are not incidental but structurally tied to the capacity and implementation issues outlined, including weak regulations and fragmented infrastructures leaving LMICs with limited leverage to enforce protections once data cross borders. For RQ3, this pattern implies that without reforms to shift control over infrastructures and contract conditions, AI-guided diagnostic and predictive tools are likely to worsen existing inequities, keeping them in the role of data suppliers and leaving individuals with only nominal control over how their health data is moved or reused.

Across all three themes, the evidence base is informative but uneven. Most of the 28 included sources are conceptual or legal-policy analyses and mapping studies that theorize how frameworks should to work rather than empirically evaluating how well they protect health data in AI implementations. Only a smaller subset provides evidence from LMIC health systems, such as qualitative case studies of specific tools or institutions (Li et al., 2024; Della Ripa et al., 2025; Olawade et al., 2026) and a few systematic reviews of AI ethics and data-sharing in developing countries (Kaushik et al., 2025; Junaid et al., 2025; Oladipo et al., 2024). Very few studies follow data flows end-to-end or measure outcomes such as successful rights enforcement, effective remedies, or demonstrable changes in vendor practices. Patient and community level perspectives are also limited compared with analyses written from the point of view of regulators, researchers or international organizations. Taken together, this means that the literature is strong on diagnosing normative gaps and governance risks, however limited on assessments of how specific regional or international frameworks perform in practice for LMIC patients and health-systems.

4. POLICY RESPONSE: Governing Cross-border Health-Data for AI in LMICs

4.1 Norms for Cross-border AI diagnostics

Evidence suggests that norms for cross-border transfers exist but are fragmented and rarely tailored to AI diagnostics. First priority is to clarify and adapt existing rules rather than invent entirely new frameworks. GDPR-style principles (lawfulness, purpose limitation, data minimization, security and strong data-subject rights) already provide a strong guideline for international health-data transfers (Bernier et al., 2024; Nwachukwu, 2025). WHO's (2021) Ethics and Governance of AI for Health similarly call for clear lawful bases, transparency, accountability and oversight of public-private partnerships using health-data across borders.

For LMICs, a realistic policy step is to issue AI-specific guidance under existing data-protection and health laws, rather than waiting for a comprehensive AI legislation. Building on the gaps identified by Munung et al. (2024), Nienaber & McKay (2024) and Wang et al. (2025) and drawing on international guidance (WHO, 2021), ministries of health/data-protection authorities (DPA) could develop guidance that:

- includes conditions for exporting health-data for AI (consent, transfer impact, assessment contractual safeguards)
- specifies expectations for model documentation, explainability and auditability in diagnostic tools
- requires Data Protection Impact Assessments/AI Impact Assessments for high-risk uses such as imaging triage/predictive risk scores.

This may have potential in terms of feasibility as case studies/legal analyses from Ghana, South Africa and Zanzibar show that existing data-protection and health frameworks can provide a starting point for regulating consent, data-sharing agreements and information security in AI-related projects, but they also emphasize substantial gaps and the need for further reform (Mensah, 2023; Donnelly, 2022; Li et al., 2024).

4.2 Strengthening Institutions and Cooperative Mechanisms

The literature highlights a gap between the institutions that are formally responsible for data protection/AI oversight and the actors actually controlling infrastructures/standards (Prinsloo & Kaliisa, 2022; Adebayo et al., 2025; Apiko & Musoni, 2025). Policy responses therefore need to reinforce existing regulators and create mechanisms for coordinated supervision across borders.

At national level, DPA, health ministries, ethics committees and medical-device regulators need clearer mandates on AI diagnostics. Studies from Nigeria and South Africa show that ethics committees and regulators are unsure how to review AI projects or allocate liability among clinicians, hospitals and vendors (Donnelly, 2022; Olawade et al., 2026). Governments can address this by:

- designating a lead authority for health-data AI
- creating joint guidance on vendor contracts, who is liable for errors and incident reporting
- ensuring that ethics committees and regulators work together so ethics review standards are consistent with data-protection and device regulations

At regional level, the AU, sub-regional economic communities and emerging regulator networks can act as central coordination points to help countries supervise AI and health data consistently. ECDPM (Apiko & Musoni, 2025) argues that EU-Africa partnerships should combine AI diagnostic pilots with shared certification processes and joint verification mechanisms such as regulatory sandboxes and regional data-sharing arrangements to ensure tools are safe and effective before getting scaled. Townsend (2025) and Hallock et al. (2021) show that federated networks and "governance-by-design" architectures work best when overseen by multi-country steering and data-access committees that set common rules for the data use. The Minerva Initiative illustrates this model with a management group acting as a data-access committee and using consent forms and Material Transfer Agreements to govern access to pooled data (Nellaker et al., 2019).

For cross-border AI diagnostics, this could mean expanding current cooperation tools such as memoranda of understanding (non-binding written agreement) between DPAs, regional model laws, ethics-committee networks into formal coordination mechanisms, such as regional health-AI tool registries, shared certification criteria for diagnostic tools, and protocols for cross-border breach reporting.

4.3 Addressing Implementation and Funding Gaps

Across the sources weak infrastructure, limited regulatory capacity and fragmented systems are the main reasons formal protections fail in practice (Hussain et al., 2025; Kaushik et al., 2025; Li et al., 2024). A policy response therefore has to treat implementation capacity and funding as core governance issues, not as secondary considerations.

First, investments in digital infrastructure and systems should prioritize privacy-preserving architectures that fit LMIC contexts. Sources on federated learning, synthetic data and trusted research environments show that it is possible to reduce cross-border transfers while still enabling multi-country AI development (Hallock et al., 2021; Arefin & Zannat, 2025; Lomotey et al., 2024). Rehan's (2025) offline-first federated mHealth framework and Li et al.'s (2024) Zanzibar experience both illustrate that context-sensitive system design including edge storage (keeping data close to created site), intermittent synchronization (system updates when Wi-Fi is available), and localized data-access rules can align data protection with service delivery in lower connectivity environments.

Second, institutions need sustained funding and training. DPAs and health regulators in Africa are under resourced and struggle to audit vendors or issue guidance (Prinsloo & Kaliisa, 2022; Munung et al.,

2024). Ethics committees report lacking AI literacy and clear standards (Olawade et al., 2026; Junaid et al., 2025). Donor and government budgets should therefore reserve dedicated allocations for:

- regulator staffing, training and technological tools for audits
- national health-data governance units that can run DPIAs, maintain data inventories and managing cross-border agreements
- evaluation studies and post-deployment monitoring of AI tools, as called for by ECDPM (2025) and Della Ripa et al. (2025).

Without this reform, tightening laws solely will not meaningfully change how data are handled in AI diagnostics.

4.4 Implications for Grand Challenges Canada and National Partners

This review suggests several tools that GCC and national teams can use to strengthen data sovereignty and individual protection in AI-guided diagnostics:

1. **Procurement-driven governance:** GCC-funded projects could be required to use standardized data-protection and transfer clauses based on emerging African guidance and GDPR guidelines that specify data-location and sub-processing chains (companies behind main vendor); mandate DPIAs/AIAs, allocate liability and guarantee patient rights (access, correction, deletion where feasible). Mensah's work on Ghana and Apiko & Musoni's ECDPM analysis both emphasize procurement and contracts as key points of influence over foreign vendors.
2. **Capacity-building alongside innovation funding:** Every AI diagnostic grant could reserve a proportion of its funds for strengthening local governance capacity via supporting DPAs, ethics committees and Ministries of Health to develop guidance, and run trainings (Prinsloo & Kaliisa, 2022; Munung et al., 2024; Olawade et al., 2026).
3. **Support for privacy-preserving, sovereign architectures:** GCC can prioritize projects that adopt federated learning, trusted research environments or data-trust models that keep identifiable data under LMIC control while enabling cross-border collaboration (Hallock et al., 2021; Lomotey et al., 2024; Rehan, 2025; Nellaker et al., 2019). Funding conditions could require local stewardship of health data and key infrastructures instead of relying on foreign companies or donors.

CONCLUSION

Cross-border health-data transfers for AI diagnostics in LMICs are already governed by global, regional and national laws/frameworks (GDPR, WHO guidance, African DP laws and emerging data-governance architectures), however, these rules form a fragmented, non-AI-specific patchwork applied unevenly. Weak infrastructure, poor data quality, limited regulatory and ethics capacity and legal uncertainty mean protections often do not reach clinical practice, while donor and vendor controlled infrastructures, minimal consent and unclear liability constrain LMIC control and individual rights. Overall, existing frameworks only partially safeguard data sovereignty and privacy. Key priorities include AI-specific guidance and impact assessments, regional oversight and certification, and investment in privacy-preserving, locally controlled architectures, alongside empirical research that traces data flows and centres around patient and community perspectives.

REFERENCES

Adebayo, A., Adura, K., Anya, E. K., & Ishola, A. V. (2025). Artificial intelligence and the future of public health surveillance in Africa and the EU. *Cognizance Journal of Multidisciplinary Studies, 5*(7), 741–746.

Adepoju, D. A., & Adepoju, A. G. (2025). Establishing ethical frameworks for scalable data engineering and governance in AI-driven healthcare systems. *International Journal of Research Publication and Reviews*, *6*(4), 8710–8726. https://doi.org/10.55248/gengpi.6.0425.1547/

Andigema, A. S., Ngnotouom Ngnokam, T. C., & Ekwelle, E. (2025). Artificial intelligence in African healthcare: Catalyzing innovation while confronting structural challenges [Preprint]. *Preprints.org*. https://doi.org/10.20944/preprints202506.1824.v1

Andigema, I., Hussain, S. A., Siddiqui, A. H., & Ndemo, B. (2025). AI in health and the coloniality of public health governance frameworks in sub-Saharan Africa? *Preprints*. https://doi.org/10.20944/preprints202503.0363.v1

Anya, A. A., Anya, K. A., Anya, E. K., & Ishola, A. V. (2025). Artificial intelligence and the future of public health surveillance in Africa and the EU. *Cognizance Journal of Multidisciplinary Studies, 5*(7), 741–746. https://doi.org/10.47760/cognizance.2025.v05i07.055

Apiko, P., & Musoni, M. (2025). *Realising the potential of AI for diagnostics in Africa: From barriers to scalability*(Discussion Paper No. 394). European Centre for Development Policy Management (ECDPM).

Arefin, S., Zannat, N. T., & Global Health Institute Research Team United States. (2025). Securing AI in Global Health Research: A Framework for Cross-Border Data Collaboration. *Clinical Medicine And Health Research Journal*, *5*(02), 1187–1193. https://doi.org/10.18535/cmhrj.v5i02.457

Bernier, A., Molnár-Gábor, F., Knoppers, B. M., Borry, P., Cesar, P. M. D. G., Devriendt, T., Goisauf, M., Murtagh, M., Jiménez, P. N., Recuero, M., Rial-Sebbag, E., Shabani, M., Wilson, R. C., Zaccagnini, D., &

Maxwell, L. (2024). Reconciling the biomedical data commons and the GDPR: three lessons from the EUCAN ELSI collaboratory. *European journal of human genetics : EJHG*, *32*(1), 69–76. https://doi.org/10.1038/s41431-023-01403-y

Davis, S. L. M., Pham, T., Kpodo, I., Imalingat, T., Muthui, A. K., Mjwana, N., Sandset, T., Ayeh, E., Dong, D. D., Large, K., Nininahazwe, C., Wafula, T., Were, N., Podmore, M., Maleche, A., & Caswell, G. (2023). Digital health and human rights of young adults in Ghana, Kenya and Vietnam: a qualitative participatory action research study. *BMJ Global Health*, *8*(5), e011254. https://doi.org/10.1136/bmjgh-2022-011254

Della Ripa, S., Santos, N., & Walker, D. (2025). AI-enabled obstetric point-of-care ultrasound as an emerging technology in low- and middle-income countries: Provider and health system perspectives. *BMC Pregnancy and Childbirth*, *25*(1), 729. https://doi.org/10.1186/s12884-025-07796-6

Donnelly D. L. (2022). First Do No Harm: Legal Principles Regulating the Future of Artificial Intelligence in Health Care in South Africa. *Potchefstroom electronic law journal*, *25*, 10.17159/1727-3781/2022/v25ia11118. https://doi.org/10.17159/1727-3781/2022/v25ia11118

Ethics and Governance of Artificial Intelligence for Health: WHO Guidance (1st ed). (2021). World Health Organization.

Ferryman, K. (2021). The Dangers of Data Colonialism in Precision Public Health. *Global Policy*, *12*(S6), 90–92. https://doi.org/10.1111/1758-5899.12953

Hallock, H., Marshall, S. E., 't Hoen, P. A. C., Nygård, J. F., Hoorne, B., Fox, C., & Alagaratnam, S. (2021). Federated Networks for Distributed Analysis of Health Data. *Frontiers in public health*, *9*, 712569. https://doi.org/10.3389/fpubh.2021.712569

Hussain, S. A., Bresnahan, M., & Zhuang, J. (2025). Can artificial intelligence revolutionize healthcare in the Global South? A scoping review of opportunities and challenges. *Digital health*, *11*, 20552076251348024. https://doi.org/10.1177/20552076251348024

Junaid, K., Nasir, M., Rafique, S., Arshad, A., Siddiqui, M., & Junaid, M. A. (2025). Ethical issues of artificial intelligence in healthcare in developing countries: A systematic review of empirical studies. *Annals of King Edward Medical University, 31*(Suppl. 2), 111–118. https://doi.org/10.21649/akemu.v31iSpl2.5827

Kaushik, A., Barcellona, C., Mandyam, N. K., Tan, S. Y., & Tromp, J. (2025). Challenges and Opportunities for Data Sharing Related to Artificial Intelligence Tools in Health Care in Low- and Middle-Income Countries: Systematic Review and Case Study From Thailand. *Journal of medical Internet research*, *27*, e58338. https://doi.org/10.2196/58338

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, T., Wandella, A., Gomer, R., & Al-Mafazy, M. H. (2024). Operationalizing health data governance for AI innovation in low-resource government health systems: a practical implementation perspective from Zanzibar. *Data & Policy*, *6*, e63. doi:10.1017/dap.2024.65

Lomotey, R. K., Kumi, S., Ray, M., & Deters, R. K. (2024). Synthetic data digital twins and data trusts control for privacy in health data sharing. In *Proceedings of the 2024 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems (SaT-CPS '24).* Association for Computing Machinery. https://doi.org/10.1145/3643650.3658605

Marey, A., Ambrozaite, O., Afifi, A., Agarwal, R., Chellappa, R., Adeleke, S., & Umair, M. (2025). A perspective on AI implementation in medical imaging in LMICs: challenges, priorities, and strategies. *European radiology*, 10.1007/s00330-025-12031-z. Advance online publication. https://doi.org/10.1007/s00330-025-12031-z

Mensah, G. B. (2024). Digital sovereignty in the age of AI: Reconciling national data control with cross-border AI innovation. *Africa Institute for Regulatory Affairs*. [Preprint].

Mensah, G. B. (2024). Ethics and privacy in AI predictive health [Preprint]. https://doi.org/10.13140/RG.2.2.36737.47207

Mensah, G. B. (2024). Protecting sensitive health data in AI-based research and development. *Africa Institute for Regulatory Affairs* [Analysis Report].

Munung, N. S., Staunton, C., Mazibuko, O., Wall, P. J., & Wonkam, A. (2024). Data protection legislation in Africa and pathways for enhancing compliance in big data health research. *Health research policy and systems*, *22*(1), 145. https://doi.org/10.1186/s12961-024-01230-7

Ndemo, B. (2025). Revolutionizing African healthcare: A systematic review of artificial intelligence and data governance. *Research Square* [Preprint]. https://doi.org/10.21203/rs.3.rs-6572611/v1

Nellaker, C., Alkuraya, F. S., Baynam, G., Bernier, R., Bernier, F. P. J., Boulanger, V., Brudno, M., Brunner, H. G., Clayton-Smith, J., Cogné, B., Dawkins, H. J. S., de Vries, B. B. A., Douzgou, S., Dudding-Byth, T., Eichler, E. E., Ferlaino, M., Fieggen, K., Firth, H. V., FitzPatrick, D. R., … Wilkie, A. O. M. (2019). Enabling global clinical collaborations on identifiable patient data: The Minerva Initiative. *Frontiers in Genetics, 10*, 611. https://doi.org/10.3389/fgene.2019.00611

Nienaber McKay, A. G., Brand, D., Botes, M., Cengiz, N., & Swart, M. (2024). The regulation of health data sharing in Africa: a comparative study. *Journal of law and the biosciences*, *11*(1), lsad035. https://doi.org/10.1093/jlb/lsad035

Nwachukwu, E., Obasi, G., & Omotayo, D. (2025). *Data Privacy and Security Concerns in AI-Driven Healthcare*.

Oladipo, E. K., Adeyemo, S. F., Oluwasanya, G. J., Oyinloye, O. R., Oyeyiola, O. H., Akinrinmade, I. D., Elutade, O. A., Areo, D. O., Hamzat, I. O., Olakanmi, O. D., Ayanronbi, I. I., Akanmu, A. J., Ajekiigbe, F. O., Taiwo, M. O., Ogunfidodo, V. M., Adekunle, C. A., Adeleke, P. O., Olubunmi, D. A., Adeogun, P. A., … Nnaji, N. D. (2024). Impact and Challenges of Artificial Intelligence Integration in the African Health Sector: A Review. *Trends in Medical Research*, *19*(1), 220–235. https://doi.org/10.3923/tmr.2024.220.235

Olawade, D. B., Clement David-Olawade, A., Aderinto, N., & Wada, O. Z. (2026). Ethical oversight of Artificial Intelligence in Nigerian Healthcare: A qualitative analysis of ethics committee members' perspectives on integration and regulation. *International journal of medical informatics*, *206*, 106140. https://doi.org/10.1016/j.ijmedinf.2025.106140

Powles, J., & Hodson, H. (2017). Google DeepMind and healthcare in an age of algorithms. *Health and Technology*, *7*(4), 351–367. https://doi.org/10.1007/s12553-017-0179-1

Prinsloo, P., & Kaliisa, R. (2022). Data privacy on the African continent: Opportunities, challenges and implications for learning analytics. *British Journal of Educational Technology*, *53*(4), 894–913. https://doi.org/10.1111/bjet.13226

Rehan, H. (2025). Bridging the digital divide: A socio-technical framework for AI-enabled rural healthcare access in developing economies. *EuroVantage Journal of Artificial Intelligence, 2*(1), 19-27.

Seddon, J. J. M., & Currie, W. L. (2013). Cloud computing and trans-border health data: Unpacking U.S. and EU healthcare regulation and compliance. *Health Policy and Technology*, *2*(4), 229–241. https://doi.org/10.1016/j.hlpt.2013.09.003

Sekalala, S., & Chatikobo, T. (2024). Colonialism in the new digital health agenda. *BMJ Global Health*, *9*(2), e014131. https://doi.org/10.1136/bmjgh-2023-014131

Serge Andigema, A., Tania Cyrielle, N. N., & Ekwelle, E. (2025). *Artificial Intelligence in African Healthcare: Catalyzing Innovation While Confronting Structural Challenges*. Public Health and Healthcare. https://doi.org/10.20944/preprints202506.1824.v1

Towett, G., Snead, R. S., Marczika, J., & Prada, I. (2024). Discursive framework for a multi-disease digital health passport in Africa: a perspective. *Globalization and Health*, *20*(1), Article 64. https://doi.org/10.1186/s12992-024-01067-3

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

Townsend, B. A., Sihlahla, I., Naidoo, M., Naidoo, S., Donnelly, D.-L., & Thaldar, D. W. (2023). Mapping the regulatory landscape of AI in healthcare in Africa. *Frontiers in Pharmacology*, *14*, 1214422. https://doi.org/10.3389/fphar.2023.1214422

Wang, X., Iftikhar, H., Hali, S. M., Shah, U., & Iqbal, M. S. (2025). Impact of health policy reforms on telemedicine and AI integration for early cancer detection among low-income populations in South Asia: A comparative policy analysis. *African Journal of Reproductive Health*, *29*(8s), 43–53. https://doi.org/10.29063/ajrh2025/v29i8s.5

World Health Organization. (2021). *Ethics and governance of artificial intelligence for health: WHO guidance*. World Health Organization. https://www.who.int/publications/i/item/9789240029200

Xia, L., Cao, Z., & Zhao, Y. (2024). Paradigm Transformation of Global Health Data Regulation: Challenges in Governance and Human Rights Protection of Cross-Border Data Flows. *Risk Management and Healthcare Policy*, *17*, 3291–3304. https://doi.org/10.2147/RMHP.S450082

Appendices

Appendix A: Search Strategy

Date of Search	**Database**	**Search Terms**	**Total # Articles**	**Articles Included in Review for Paper**
2025-11-07	Scopus	**String 1** TITLE-ABS-KEY(("artificial intelligence" OR "AI" OR "machine learning") AND (diagnostic* OR imaging OR "clinical decision support" OR "decision-support") AND ("health data" OR "medical data" OR "patient data") AND ("cross-border" OR "cross border" OR "transborder" OR "international transfer*" OR "data transfer*" OR "data flow*") AND (framework* OR "data protection" OR "data governance" OR "privacy law" OR "privacy regulation" OR regulation* OR governance)) AND (LMIC* OR "low- and middle-income countr*" OR "low and middle income countr*" OR Africa* OR "Sub-Saharan Africa" OR "Global South") **String 2** TITLE-ABS-KEY(("artificial intelligence" OR "AI" OR "machine learning") AND (diagnostic* OR imaging OR "clinical decision support") AND ("health system*" OR "health service*" OR "healthcare" OR hospital*) AND ("data protection" OR "data privacy" OR "personal data" OR "patient privacy" OR "data security") AND (effectiveness OR evaluation OR impact OR implementation OR "case stud*" OR "lessons learned") AND ("cross-border" OR "cross border" OR "international" OR "transnational" OR "data sharing")) AND (LMIC* OR "low- and middle-income countr*" OR "low and middle income countr*" OR Africa* OR "Sub-Saharan Africa" OR "Global South")	String 1: 3 String 2: 7	**String 2** 1. Synthetic Data Digital Twins and Data Trusts Control for Privacy in Health Data Sharing 2. Federated Networks for Distributed Analysis of Health Data
2025-11-07	PubMed	**String 1**	String 1: 2	**String 1**

		(("artificial intelligence" OR "machine learning" OR AI) AND (diagnostic* OR imaging OR "clinical decision support" OR "decision-support") AND ("health data" OR "medical data" OR "patient data") AND ("cross-border" OR "cross border" OR international OR "data sharing" OR "data transfer*" OR "data flow*") AND ("data protection" OR "data privacy" OR "personal data" OR "privacy law" OR "data governance")) AND (LMIC* OR "low- and middle-income countr*" OR "low and middle income countr*" OR Africa OR "Sub-Saharan Africa" OR "Global South") **String 2** (("artificial intelligence" OR "machine learning" OR "AI") AND (diagnostic* OR imaging OR "clinical decision support") AND ("health system*" OR "health service*" OR healthcare OR hospital*) AND ("data protection" OR "data privacy" OR "patient privacy" OR "personal data" OR "data security") AND (effectiveness OR evaluation OR impact OR implementation OR "case stud*")) AND (LMIC* OR "low- and middle-income countr*" OR "low and middle income countr*" OR Africa OR "Sub-Saharan Africa" OR "Global South")	String 2: 20	1. Enabling Global Clinical Collaborations on Identifiable Patient Data: The Minerva Initiative 2. Reconciling the biomedical data commons and the GDPR: three lessons from the EUCAN ELSI collaboratory **String 2** 3. Mapping artificial intelligence adoption in hepatology practice and research: challenges and opportunities in MENA region 4. Ethical oversight of Artificial Intelligence in Nigerian Healthcare: A qualitative analysis of ethics committee members' perspectives on integration and regulation 5. AI-enabled obstetric point-of-care ultrasound as an emerging technology in low- and middle-income countries: provider and health system perspectives
2025-11-09	Google Scholar	1. "artificial intelligence" diagnostic* "health data" "cross-border" "data protection" framework LMIC OR Africa 2. "artificial intelligence" diagnostic* "data protection" evaluation implementation "low- and middle-income countries" 3. ("artificial intelligence" OR AI) AND (health OR healthcare OR "health system*" OR "health data") AND ("data protection" OR "data privacy" OR "data governance" OR "data security" OR "personal data") AND (Africa OR "Global South" OR LMIC* OR "low- and middle-income countr*" OR "developing countr*" OR "low-resource setting*" OR "low-	1. 815* (60) 2. 2880* (70) 3. 17600* (40) *complete output; articles were reviewed by relevan	1. Securing AI in Global Health Research: A Framework for Cross-Border Data Collaboration 2. Realising the potential of AI for diagnostics in Africa: From barriers to scalability 3.Operationalizing health data governance for AI innovation in low-resource government health systems: a practical implementation perspective from Zanzibar 4. ETHICS AND GOVERNANCE OF ARTIFICIAL INTELLIGENCE FOR HEALTH (WHO GUIDANCE)

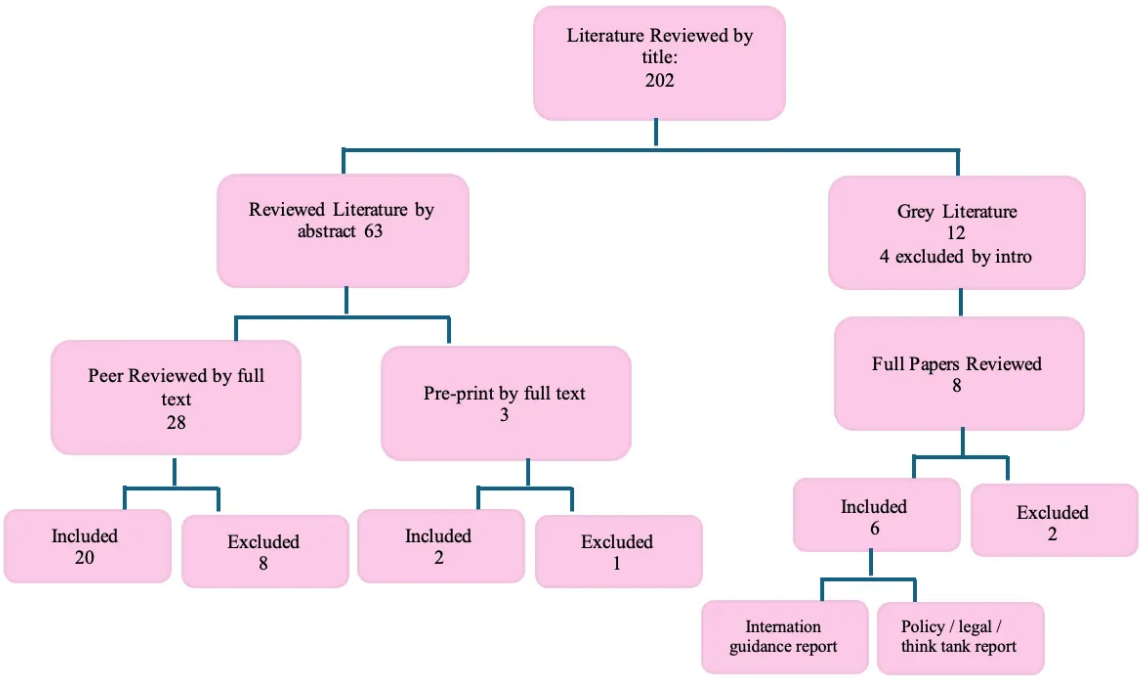
		resource healthcare") AND (framework OR governance OR regulation OR policy OR ethics OR "ethical issues")	cy order and when no article was relevant in one page, searching was stopped; number in parentheses reflect the number titles reviewed)	5. Can artificial intelligence revolutionize healthcare in the Global South? A scoping review of opportunities and challenges 6. Impact and Challenges of Artificial Intelligence Integration in the African Health Sector: A Review 7. Impact of health policy reforms on telemedicine and AI integration for early cancer detection among low-income populations in South Asia: A comparative policy analysis 8. Ethical Issues of Artificial Intelligence in Healthcare in Developing Countries: A Systematic Review of Empirical Studies 9. Mapping the regulatory landscape of AI in healthcare in Africa 10. Artificial Intelligence in African Healthcare: Catalyzing Innovation While Confronting Structural Challenges 11. Governance-by-Design as an Enabler of AI in Digital Health in Sub-Saharan Africa 12. Discursive framework for a multi-disease digital health passport in Africa: a perspective 13. Digital Sovereignty in the Age of AI: Reconciling National Data Control with Cross-Border AI Innovation 14. ARTIFICIAL INTELLIGENCE AND THE FUTURE OF PUBLIC HEALTH SURVEILLANCE IN AFRICA AND THE EU 15. Establishing Ethical Frameworks for Scalable Data Engineering and

				Governance in AI-Driven Healthcare Systems. 16. The regulation of health data sharing in Africa: a comparative study 17. protecting sensitive health data in AI based research and development 18. Data Privacy and Security Concerns in AI-Driven Healthcare 19. Challenges and Opportunities for Data Sharing Related to Artificial Intelligence Tools in Health Care in Low- and Middle-Income Countries: Systematic Review and Case Study From Thailand 20.Revolutionizing African Healthcare: A Systematic Review of Artificial Intelligence and Data Governance 21. Data privacy on the African continent: Opportunities, challenges and implications for learning analytics 22. Ethics and Privacy in AI Predictive Health 23. First Do No Harm: Legal Principles Regulating the Future of Artificial Intelligence in Health Care in South Africa 24. Data protection legislation in Africa and pathways for enhancing compliance in big data health research

Appendix B: Inclusion/Exclusion criteria

Dimension	**Include**	**Exclude**
Article type	Peer-reviewed articles; conference articles; preprints (given the novelty of this topic, preprints were considered); reports and guidance from international organizations and policy / legal bodies	Web pages, news articles, opinion pieces, blogs, and advocacy reports
Methodology	Qualitative or quantitative empirical studies; legal / policy / ethical analyses; comparative regulatory studies; case studies and implementation reports that discuss governance of health data or AI.	Technical AI performance or algorithm papers with no discussion of governance, regulation, data protection, or cross-border transfers
Geographic Scope	Studies focused on LMICs; multi-country / regional / global frameworks (GDPR, WHO AI guidance, AU data protection) where at least one implication for LMICs / South-North data flow is analyzed	HIC only studies that do not address cross-border transfers, collaboration with LMICs, or translational relevance for LMIC data governance
Sector	Health sector, digital health, AI diagnostics/imaging, and broader personal-data governance domains when they directly analyze cross-border or sensitive-data rules that are applicable to health-data transfers.	Non-health sectors with no clear relevance to governance of health or health related personal data
Time frame	2020-2025; surge in AI diagnostics. A small number of pre 2020 governance texts may be cited for background but were not part of the formal screened sample	Before 2015

Appendix C: Decision tree



Appendix D: Data Extraction Table (example from 2 sources)

Citation	Country/region	AI tool/health context	Governing framework mentioned	Key findings	Study Type
Munung et al. (2024) ; TITLE: Data protection legislation in Africa and pathways for enhancing compliance in big data health research	37 African countries	Big data health and genetic research	National data protection; African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention); GDPR as a comparator	Health/genetic data are treated as sensitive and protected by data protection principles, but rules for secondary use and international transfer are ambiguous / inconsistent across countries creating compliance issues for African researchers,	Comparative policy analysis; peer reviewed article

				weakens African states' data sovereignty. They suggest harmonized safe data flow mechanisms (trusted environments, consent, codes of conduct)	
World Health Organization (2021) - TITLE: Ethics and Governance of Artificial Intelligence for Health: WHO Guidance	Global but attention to implications for LMICs	Broad AI for health, including diagnostics, predictive tools, decision support, and public health applications	International human rights law; data protection and health data laws; bioethics principles	- Sets six core principles: protect autonomy, promote well-being, safety and public interest, ensure transparency, promote responsibility and accountability, ensure inclusiveness and equity, promote responsiveness and sustainability. - Warns that AI can worsen bias, surveillance and digital divides in LMICs. Identifies gaps in privacy, consent, transparency, accountability and benefit sharing, and mentions that control over health data and AI infrastructures may concentrate in big private actors and HIC unless LMICs build their own governance capacity and negotiate fairer arrangements.	policy report; grey literature