Protecting Stigmatized Health Data: An Evaluation of Data Protection in AI-Based Healthcare Technologies in Senegal

Isabella Miller

Student #:101180343

Norman Paterson School of International Affairs, Carleton University

INAF 5706: Global Health Policy

Dr. Valerie Percival

November 27, 2025

Word Count: 6,433

When you die, where does your data go? The invention of artificial intelligence (AI) has changed the privacy and data protection landscape. Traditional data protection regulations stipulate that individuals reserve the right to revoke access to their data, but once data is input into AI-models, it can never be scrubbed entirely. The integration of AI-based technologies in healthcare raises ethical concerns about privacy in health data collection, widely acknowledged to be some of the most personal information recorded about an individual during their lifetime.

Research Question and Roadmap

What mechanisms are available to ensure data privacy and security of patients with stigmatized illnesses during their interactions with an AI-based health intervention? This review will evaluate the existing status of data protections in Senegal, analysing how the rights to one's own data changes through their lifetime, and what it means to consent to have health data fed to AI-based healthcare technology. These rights will be assessed by examining what data is collected during a patient's interaction with an AI-based healthcare system, how the collected data is protected, and what are the consequences if the data were to be breached. To properly illustrate these consequences, this review specifically evaluates the experience of patients with HIV, a highly stigmatized diagnosis in Senegal. Enforcement measures are used as a metric to evaluate the efficacy of Senegal's data protection and cybersecurity policies.

This review begins with a description of the methodology for selecting the included records. The literature review was conducted looking at four topics: 1) data protection and individual privacy rights, 2) AI and health data, 3) data breach and enforcement, and 4) data protection policies. Each topic will be broken down in the discussion section where they are applied to the case of an individual with a stigmatized diagnosis, HIV, in Senegal. The review will conclude with identifying research and policy gaps and make recommendations for ethically integrating AI-based technologies in health systems.

Data Protection and Individual Privacy Rights

First this review will address who holds the rights to health data and what informed consent means in the context of health data collection. It will then attempt to delineate at what point the communal good overpowers an individual's right to data privacy and protection.

AI and Health Data

Next, the rights of the individual will be contextualized by asking what health data is collected from patients, and how AI-based healthcare technologies are being integrated in Senegal.

Data Breach and Enforcement

The review will then discuss the consequences of a data breach, what safeguarding mechanisms can be built into AI-based healthcare technologies to ensure data protection, the enforcement mechanisms available to an individual if their right to privacy has been violated, and who is held accountable by these enforcement mechanisms.

Data Protection Policy Response

Finally, this review will critically examine Senegal's existing data protection and privacy laws against the current gold standard of data protection regulation, the European Union's General Data Protection Regulation (GDPR). It will conclude with policy recommendations for future regulation of AI-based healthcare technologies.

Key Terms

Privacy is defined as the exclusion of others from personal affairs, the ability to keep personal information to oneself (Makulilo, 2024). A data owner is understood as the individual who has the autonomy to consent to data collection and therefore makes decisions for their data protection. The data subject in the individual to which the information pertains.

AI-based healthcare technologies refer to models that would use and store individual patient data necessary for a standard interaction with a healthcare provider. This includes AI appointment transcription services, diagnostic tools, chatbots, and administrative systems. It excludes research or mapping technologies because the data used is often anonymized or inherently does not contain identifying information. Although health data can be deanonymized, this review focuses on the risk of sensitive patient data being breached because of the expectation of privacy when giving a healthcare provider sensitive information.

Methods

The scope of this review is based on the article “The Right to Be Forgotten Is Dead: Data Lives Forever in AI” (Higa, Bedikian, & Costa, 2025) that was selected during the initial literature review for Stage 1 of the policy proposal for Grand Challenges Canada. Senegal was determined to be a region of interest for Grand Challenges Canada and also has comprehensive literature evaluating its data protection regulations.

Sources of Information

I conducted searches for relevant literature published between 2020 and 2025 that was available on the Omni, Google Scholar, PubMed, Science Direct, and JSTOR databases. Papers were limited to this time period to reflect the post COVID-19 healthcare research boom, that corresponds with the emergence of AI-based healthcare technologies.

Policy and legislation that was referenced in these works was later searched, using the most updated version. Some legislation pre-dates 2020 but are still included because they are the current laws in Senegal. These materials were gathered from the official Commission de Protection des Données Personnelles du Sénégal[1] (CDP) website using manual searches.

Search Strategy

The following search terms were used: “AI health” AND “Senegal” AND “data protection”, “AI health” AND “data protection”, “data protection” AND “AI healthcare”, “data protection” AND “Senegal”, “data protection” AND “enforcement” AND “Senegal”, “data collection” AND “Senegal” AND “HIV” AND “data protection”, “AU Convention on Cybersecurity” AND “Senegal”, “AU Convention on Cybersecurity” AND “Senegal” AND “health”, “data collection” AND “Senegal” AND “HIV” AND “stigma”.[2]

A manual search was conducted to find the age of consent for medical decision in Senegal using the search string "health" AND "age of consent" AND "Senegal" on Google Scholar.

Selection Criteria

Accepted article types included peer-reviewed, from international organizations with a review process, grey-literature, reports, country evaluations, and policy. News articles and opinion pieces were excluded. Records were only included if they were accessible and not paywalled. Studies conducted with both qualitative and quantitative methodologies were included. Records focusing geographically on low-middle income countries, specifically Senegal, and the European Union (specifically if referencing the GDPR) were included. The GDPR is widely recognized as the gold standard for data privacy and security regulation, and is included as a comparison for Senegalese regulations; it also provides a regulatory framework in which to centre the development of Convention 108. Records studying middle-high income

---

[1] Commission of Personal Data Protection of Senegal

[2] See Appendix A for the complete Search Strategy results and notes.

countries were excluded because of the difference in data sovereignty concerns and the resources available to implement AI-based healthcare models. Records that only assessed data protection considerations through America's Health Insurance Portability and Accountability Act (HIPAA) were excluded because HIPAA applies only to healthcare providers in the United States and does not focus on digitalization of data.

All results were filtered by year to only include 2020–2025. Google Scholar searches were filtered to exclude citations. Science Direct searches were filtered to only include review articles, research articles, encyclopedia, book chapters, and case reports. JSTOR searches were filtered to only include journals, book chapters, and research reports.

Figure 1

Inclusion and exclusion criteria chart

	Included	Excluded
Article Type	• Peer reviewed • International organizations with review process • Grey-literature • Reports • Country evaluations • Policy	• News articles • Opinion pieces • Paywalled articles
Methodology	• Qualitative studies • Quantitative studies	
Geographic Scope	• Low-middle income countries • Areas of interest for GCC o Senegal • European Union o GDPR as standard for data protection	• Middle-high income countries • United States of America o HIPAA focused
Time Frame	• 2020 to current o Unless existing legislation predates 2020	• Pre-2020

I assessed each title and abstract with the following criteria: (1) was the paper written between 2020 and 2025, (2) did the article describe how AI-based healthcare systems are being implemented, or ethical concerns with data protection in AI-based healthcare systems, or repercussions of data breaches, (3) did the paper focus on AI-based healthcare applications in low income countries, (4) if the paper focused on Africa, was Senegal included, and (5) if the paper discussed stigma surrounding HIV, did it include issues with data collection and protection?

Results of the Search for Source Material

I used Microsoft Excel to remove duplicate articles and organize the collected data. A total of 87 records were collected from the initial search parameters and selection criteria listed above. After removing duplications, 81 records remained. Each record's abstract was screened for relevance, leaving 70 records to assess for full-text eligibility. Forty nine records met the inclusion criteria to be included in this literature review.[3]

Manual searches were conducted to generate additional sources pertaining to the age of consent for patients to make their own health decisions in Senegal. A manual search of the CDP website provided full-text versions of Senegal's 2008 and 2016 data protection legislations as referenced in the selected records. The Senegalese Penal Code and data protection legislation was searched to note the year of adoption, but because the official text is in French, therefore these documents were not considered records.

Records that met the inclusion criteria but were removed for full-text ineligibility were found to be too broad in their description of AI-based health systems or in their policy recommendations to the extent that they could not meaningfully contribute to the literature review. If a record focused on the digitalization of health data for research purposes rather than patient interactions it was excluded. Records were excluded if they vaguely discussed data protection and privacy standards in e-health interventions without specifically outlining the

---

[3] See Appendix B for the complete Article Inclusion Process.

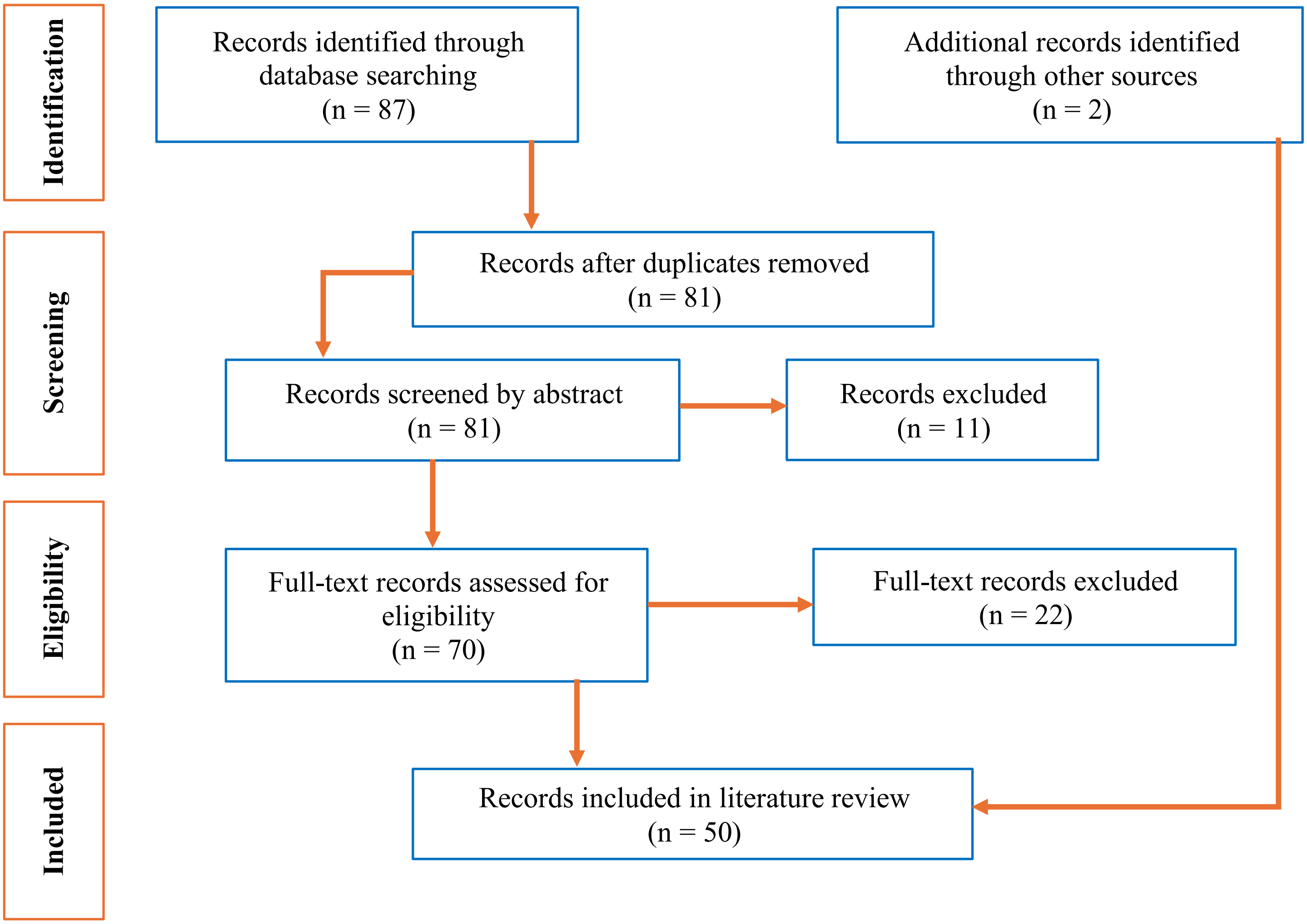
mechanism for compliance. As the scope of the review narrowed, records were excluded if they evaluated healthcare interventions unrelated to HIV, unless they considered patient privacy in health data collection. Many broadly commented on legislative developments in sub-Saharan Africa legislative developments but did not reference Senegal outside of their ratification of the Budapest Convention and/or the African Union Convention on Cybersecurity and Personal Data Protection.

Limitations

Searches were conducted in English, which may exclude relevant literature from non-English academics, official Senegalese documents in French, or articles which use “Sénégal”. Literature behind a paywall was inaccessible and therefore excluded, but may still be relevant. News articles and opinion pieces that were excluded may include a perspective on Senegal’s data protection legislation and enforcement mechanisms that was not captured by academics or official government sources.

Figure 2

The screening and selection process decision tree



Literature Review

Three major themes were adduced from the records: data ownership rights are underdeveloped, patients and healthcare providers have concerns about the protection of health data in AI models, and existing enforcement mechanisms are insufficient to hold actors accountable for data breaches.

Data Ownership Rights are Underdeveloped

Data owner's rights are cardinal to data protection, as the data owner decides who and what can collect their data and how their data is used.

Data Ownership and Custodianship

Data ownership is assumed to coincide with the age of consent for medical decisions, which in Senegal is 14 (Rosen, Stone, & Mbizvo, 2023). Parental consent to medical procedures would be necessary before the individual is 14. Custodianship of a data subject removes their autonomy, making the parent the data owner to data that is not their own. Some patients believe their family members should be involved in the data ownership decision (Bavli, Ho, Mahal, & McKeown, 2025). Amini et al. suggests that data subjects may extend to include biological family members because biometric medical data may correspond with the data owner (2023). Their review indicates that data ownership must be defined more rigidly in regulations concerning AI-based healthcare technologies because the implications of allowing data collection are complicated by the opaqueness of AI systems (Amini, et al., 2023).

Informed Consent

In a strictly medical context, informed consent means the patient is wholly aware of the extent and results of the proposed medical intervention and is accepting associated risks. In AI-based healthcare technologies, the patient should be able to consent before disclosing their data, and the algorithm should be adjusted to respect the patient's boundaries (Lalwani, et al., 2024).

Informed consent becomes more difficult if the AI model uses black-box algorithms, highly complex machine learning techniques that the healthcare provider would not be able to understand to relay to the patient (Gerke, Minssen, & Cohen, 2020). Some interventions like chatbots prompt the patient to agree to a user agreement that can be lengthy, technically complex, and contain a clause that data use by the model can update with software changes (Nwachukwu, Obasi, & Omotayo, 2025). These user agreements do not meet the standards of informed consent but are permitted for the release of health data (Gerke, Minssen, & Cohen, 2020).

Currently, the lack of regulations allows for data sharing between healthcare providers and publicly accessible servers where actors can access patient data for secondary uses (Moulaei, Akhlaghpour, & Fatehi, 2025). Algorithmic fairness and transparency should be prerequisites to patients giving informed consent to their data being collected.

The Individual Versus Communal Good

An ethical challenge in healthcare is understanding when individual rights need to be set aside for the good of a larger group. Processing health data is generally prohibited in data protection regulations, per Article 9(1) of the GDPR. This can be waived if the data subject has given explicit consent or where "the processing is necessary for reasons of public interest in the area of public health" (Gerke, Minssen, & Cohen, 2020). During the COVID-19 pandemic, governments issued guidelines for modified data protection including that data can be processed strictly for the purpose of combatting the virus and its storage should only last for the duration of the pandemic (Ilori, 2020). These guidelines circumvented existing data protection regulations and created legal vacuums where data owners lost their rights.

Another dimension to data ownership and public good is the availability of data collected and stored by private entities: some patients believing their anonymized data should be accessible to researchers to further medical advancements (Bavli, Ho, Mahal, & McKeown, 2025). Ownership becomes muddled by commercial utilization and private storage of data, specifically with cloud-hosted algorithms where the storage model architecture and parameters are hidden (Dziedzic, Issa, Chaurasia, & Tanasiewicz, 2024; Khalid, Qayyum, Bilal, Al-Fuqaha, & Qadir, 2023).

Odero, Nderitu, and Samuel offer a different perspective: the *Ubuntu* way, which promotes community and collective wellbeing through inter-connectedness (2024). This philosophy suggests that individualism in data protection may not be prioritized over data disclosure for increased research participation.

Concerns About AI Models Collecting Sensitive Health Data

African countries are using AI applications in medical record management, access to information, monitoring chronic disease, sharing information between healthcare providers, administrative management, and research to reduce infant and maternal mortality rates (Kiemde & Kora, 2020). However, there is resistance to adopting this technology because of a lack of trust: as reliance on the healthcare system increased, patients were less likely to trust the privacy of AI data (Zahlan, Ranjan, & Hayes, 2023).

What Data is Collected?

Patients and healthcare providers alike have concerns about the security of AI-based health technologies, specifically with data breaches and how the data is stored and transmitted (Bavli, Ho, Mahal, & McKeown, 2025). Data that typically would be collected in an individual's health record includes information on their health status, medical history, payment for healthcare services, demographic details, and general personal identifying information (Nwachukwu, Obasi, & Omotayo, 2025). Models that have direct integration with electronic health records are given all the patient's sensitive data to assist the physician with treatment options, drug interactions, and improving administrative efficiency (Nwachukwu, Obasi, & Omotayo, 2025). Chatbots or other therapeutic systems collect clinical data for behavioural assessments, and may record physician notes and/or patient responses (Nwachukwu, Obasi, & Omotayo, 2025). This data is highly sensitive and may be stigmatized, with personal consequences if the data were to be disclosed non-consensually.

It is a sensitive balance between protecting the patient's data and ensuring that the AI model can function as intended to support the patient or physician (Dziedzic, Issa, Chaurasia, & Tanasiewicz, 2024). Algorithms and safeguards are proprietary: privacy-preserving machine learning techniques are designed for specific algorithms, and cannot be widely applied to all AI-based healthcare technologies (Khalid, Qayyum, Bilal, Al-Fuqaha, & Qadir, 2023). Limited applications allow the data owner to edit or delete the data that was shared once it has been submitted to the algorithm (Yener, Chen, Gumusel, & Bashir, 2025).

AI-Based Healthcare Technologies Being Integrated in Senegal

The digitalization of healthcare is championed as a strategy for improving Senegal's economic growth and actualization of the Sustainable Development Goals. AI-based healthcare technologies are being introduced to reduce administrative burden and enhance patient access in remote areas: AI chatbots were used to answer questions and combat false information during the COVID-19 pandemic (Heng, Tsilionis, Scharff, & Wautelet, 2022). Ndiaya et al. find that there is hesitancy in providing personal information over the internet in Senegal, perhaps hindering widespread adoption of digital healthcare services (2025).

Insufficient Enforcement Mechanisms for Data Breaches

Data breaches include both data exploitation where health data is used for secondary purposes outsides of what patients consented to an cyberattacks by malicious actors. Healthcare data systems are not infallible. In 2021, up to 45 million Americans were affected by healthcare cyber-attacks according to the US Department of Health and Human Services (Bavli, Ho, Mahal, & McKeown, 2025).

Personal Consequences of a Data Breach

Personal consequences of a data breach are barriers to the adoption of AI-based healthcare technologies. Aside from traditional concerns of identifying information being shared, patients report fears of possible blackmail, loss of employment, or social ostracization as a result of health information being released (Khalid, Qayyum, Bilal, Al-Fuqaha, & Qadir, 2023). Data exposure only accounts for 4% of the major cybersecurity attacks in Senegal between 2005–2023, but these were ransomware attacks which held data hostage which are particularly detrimental if health systems are targeted (Sall, 2024).

Constructing AI Models with Safeguards

Data used in AI-based healthcare technologies is particularly vulnerable because it can be accessed both through the algorithm and data storage centres. Through the algorithm, attackers can access patient information by reconstructing the data an AI model was trained on (Nwachukwu, Obasi, & Omotayo, 2025). To promote general data protection, security and privacy training can establish best practices for healthcare providers to use technologies responsibly. Institutions can enact clear security requirements for providers such as designating acceptable devices to access health data or multifactor authentication processes (Moulaei, Akhlaghpour, & Fatehi, 2025).

To prevent the download of sensitive data, models can integrate robust authentication processes and anonymization techniques including pseudonymized patient data or quasi-identifiers like birthdate and gender (Moulaei, Akhlaghpour, & Fatehi, 2025). Blockchain is an innovative security solution proposed to limit outside access to medical data while allowing for standardized data flows between healthcare providers (Ba, et al., 2025). Hosted locally, a blockchain provides Senegal with more direct management over the entities authorized to access health data (Ba, et al., 2025). Relating to data owner consent, algorithms can be created with purpose limitations specifying what the data can be used for (Salami, 2024). Data minimization protocols can ensure that the AI model is not collecting more information than is strictly necessary to complete the task (Salami, 2024). Encryption and security is further complicated if the AI-based healthcare technology integrates wearable systems to monitor patient health and data because the communication between the device and AI model requires Bluetooth or internet access, creating more access points for attackers (Charfare, Desai, Keni, Namiar, & Cherian, 2024). The World Health Organization recommends holistic risk management to continuously assess risk throughout modifications made to machine learning models as it collects data (2023).

Cloud storage remains a risk to data protection because of regulatory challenges between competing jurisdictions (Salami, 2024). Digital sovereignty can promote data protection if the data centres are localized and therefore subject to domestic legislation: however, digital sovereignty can be difficult to achieve due to limited resources, infrastructure, and technical capabilities (Ayana, et al., 2024). Senegal is prioritizing technological education in their curriculums, with academies like SONATEL training students in programming and coding which can help establish digital sovereignty (Kiemde & Kora, 2020). Cables and other infrastructure-building investments are being made between African states and American or Chinese corporations in pursuit of sovereignty (Fidler, 2023). Building a datacentre with Huawei, Senegal is a leader in data onshoring, but by achieving this through Chinese private investments the datacentre is open to espionage and surveillance risks (Soulé, 2024).

Enforcement for Privacy Right Violations

International human rights law provides a universal framework for the right to privacy, but the national legislation of many states is inadequate and fails to meet international standards for enforcement (Oganesian, 2020). Many African countries have adopted major principles and provisions relating to data subject's rights modelled off the GDPR, considered to be the gold standard in data protection regulation (Ademuyiwa & Adeniran, 2020).

Senegal ranks in the top five African countries for efficacy of rule of law and regulatory enforcement of data protection laws (Ademuyiwa & Adeniran, 2020). Senegal's Cybercrime Law criminalizes unlawful actions aimed at gaining access to digital systems with the intent of obtaining data. It follows the CIA triad of principles for security policies: confidentiality, integrity, and availability (Mabunda, 2025). However, the language of the legislation is open to interpretation and causes gaps in effective enforcement (Mabunda, 2025).

Private corporations are not often held accountable for data breaches. Accountability and liability are difficult to assign because of the lack of regulatory framework for AI use in healthcare (Mohammed & Malhotra, 2025). Without regulatory frameworks, patients are only protected by the AI manufacturers' privacy and accountability policies which they may purposefully complicate to deter patients from seeking legal recourse (Mohammed & Malhotra, 2025). Accountability can be improved with public-private partnerships aiming to introduce private-sector innovations in public applications (Alami, et al., 2025). Tripartite partnerships include patients or data subjects as partners equal to the private entity and public organization, which ensures the perspectives of civil society are integrated in risk mitigation for data protection in AI models (Alami, et al., 2025).

Research Gaps

The entire study of the preservation of data protection rights in AI-based healthcare technologies in Senegal is hypothetical. Because AI-based healthcare technologies are so new, the true risks to data protection are unknown. AI models are in their infancy, but are evolving rapidly beyond the scope of any current or proposed legislation. The true consequences of a data breach are unknown because they have not yet occurred. Large gaps remain in assigning liability for harms resulting from data breaches of AI-based healthcare technologies. More research needs to be done after these interventions have been implemented for a significant enough amount of time to study the benefits and obstacles to providing healthcare with AI-based technologies.

A significant gap remains in defining data ownership. This would need to include any regulations updated to directly address the use of AI in collecting and storing health data. If parental consent is required for data collection before an individual reaches the age of maturity for medical decisions, are they able to then renege access to the data that was previously given? Or, perhaps is the individual, as the data subject, not the data owner until the age of maturity at which point they decide how future data will be collected. It is also important to determine when data ownership ends; in end-of-life healthcare interactions, is the data owner whoever holds power of attorney over the data subject, or would the data subject make designations for their data in a will? Does data ownership end with the passing of the data subject, or does it transfer to living biological relatives? Could data subjects pledge their data to research, much like organ donors? These legal considerations are necessary to establish a robust data protection strategy that addresses the right to be forgotten.

Discussion

To contextualize the concerns of patients, this review will illustrate the consequences of a data leak from a hypothetical AI-based healthcare technology revealing an individual's HIV diagnosis in Senegal.

Stigmatized Diagnoses: A Case Study of HIV in Senegal

HIV health data is considered to be the most sensitive information to a data subject because of the stigmatization associated with an HIV/AIDS diagnosis (Makulilo, 2024). The exposure of stigmatized diagnoses is one of the main identified risks of integrating AI-based healthcare technologies (Nwachukwu, Obasi, & Omotayo, 2025).

Stigma in disclosure of HIV status comes from the behaviours associated with contracting the condition and its prevalence in certain communities; 6.6% of female sex workers, 5.2% of injecting drug users, and 27.6% of men who have sex with men (MSM) are estimated to have HIV in Senegal (Ndione, et al., 2022). Article 319 of the Penal Code criminalizes homosexual sexual practices, levying a maximum jail sentence of 5 years or CFAF 1,500,000 fine (Ndione, et al., 2022). Patients rely on the confidentiality of their healthcare providers to access treatment and receive care indiscriminately. The addition of AI-based administrative technologies for appointment transcription or patient management might dissuade MSM from seeking treatment. MSM who had disclosed their sexual practices to both family and healthcare providers were more likely to avoid seeking care due to the possibility of someone learning their sexual status through gossip (Dibble, et al., 2022). Five percent of respondents in Senegal reported their status being disclosed without their consent (Friedland, et al., 2020). If the confidentiality of healthcare providers cannot be trusted, AI models with opaque security practices will not contribute to more MSM seeking treatment.

AI-based healthcare technologies like chatbots offer unique solutions to problems of stigma due to their lack of face-to-face interaction, but carry their own security problems. Lack of privacy laws for health data protection can deter testing and treatment. Senegal's data protection law states that personal data should not be used to the disadvantage of individuals or groups, protecting data subjects in data processing for research (Munung, Staunton, Mazibuko, Wall, & Wonkam, 2024). It notably does not have a provision for data subjects to request the deletion or removal of their data, nor is there a compensatory clause if the data subject suffers harm from violations of their data protection rights (Munung, Staunton, Mazibuko, Wall, & Wonkam, 2024). If a data subject were to attend a clinic and request HIV testing but receive a negative test, they would not be able to remove their data from the AI model. This regulatory gap creates further fear that their HIV status may be released to a third-party without their knowledge (Makulilo, 2024). Thirteen percent of individuals with their HIV status disclosed reported experiencing harassment, exclusion from social, religious or familial events, blackmailing, and/or refusal of employment opportunities (Friedland, et al., 2020).

Combatting stigma is the primary method for improving healthcare access for patients diagnosed with HIV. Friedland et al. identifies the Stigma Index 2.0 as an advisory system to ensure indiscriminate healthcare treatment (2020). AI-based healthcare technologies should be scrutinized with the same rigour as traditional health interventions, especially when they are implemented in vulnerable populations like those with stigmatized diagnoses.

Policy Responses

International Policy Responses

Instruments such as the GDPR, Convention 108, and Budapest Convention provide recommendations for formulating robust data protection regulations. Since Africa has been trailing in the development and adoption of AI systems, states are vulnerable to ethics-dumping from Western states with established data protection regulations for AI-based healthcare technologies (Odero, Nderitu, & Samuel, 2024).

The General Data Protection Regulation (GDPR)

The GDPR sets a high bar for data protection regulations, one that is ambitious but unattainable (Mantelero, 2021). It reflects a European regulatory framework that might be incompatible with domestic data protection cultures (Mantelero, 2021). Health data is defined as sensitive and strict conditions apply to the use of AI models in medicine (Moreno-Sénchez, Del Ser, van Gils, & Hernesniemi, 2025).

Introduced in 2018, the GDPR applies to organizations operating in the European Union or using the data of their citizens. Failure to comply with the GDPR may result in significant fines. Article 6 of the GDPR provides the right to explanation that should include the rationale behind decisions made by AI models, but this is complicated by black-box systems and proprietary algorithms (Mohammed & Malhotra, 2025; Moreno-Sénchez, Del Ser, van Gils, & Hernesniemi, 2025). The GDPR places an onus on healthcare providers to be transparent with their patients about the use of AI in their service provision (Gerke, Minssen, & Cohen, 2020). Article 33 requires healthcare organizations to notify data subjects of a data breach within 72 hours (Mohammed & Malhotra, 2025). Many AI application system providers do not include notification of data breach in their user agreements or privacy policies (Yener, Chen, Gumusel, & Bashir, 2025). Senegal does not require or provide notification for data breaches (Ilori, 2020). While states should strive to implement data protection policies similar to the GDPR, Convention 108+ may provide more realistic standards and is therefore more likely to be adopted (Mantelero, 2021).

To address accountability gaps in the GDPR, in 2024 the European Union adopted Regulation 2024/1689, the first comprehensive legal framework on AI (Turinici, Petcu, & Paraschiv, 2025). This regulation strengthens existing data protections and standardizes the application of AI-based healthcare technologies (Turinici, Petcu, & Paraschiv, 2025).

Convention 108+

Senegal acceded to the Convention on the protection of individuals with respect to the processing of personal data (Convention 108). Convention 108 is the first binding international instrument that protects individual rights during data collection and processing and regulates cross-border flow of personal data (Oganesian, 2020). The Organisation Internationale de la Francophonie fostered collaboration between French speaking countries, prompting Senegal to sign Convention 108 (Mantelero, 2021). It has been modernized to Convention 108+ to better align with the GDPR (Slokenberga, 2020). Senegal must review their data protection laws to meet the adequacy requirements of Convention 108+ (Slokenberga, 2020). Joining Convention 108+ legitimizes African states in their data protection and creates avenues for trade relationships with the European Union (Greenleaf & Cottier, 2022).

The Malabo Convention

Africa is the first regional union outside of Europe to adopt a data protection Convention (Greenleaf & Cottier, 2022). The African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention) places emphasis on consent as a legal basis for data processing (Salami, 2024). It takes from the GDPR privacy principles and definitions such as data quality, limited usage, security, access, and correction (Greenleaf & Cottier, 2022). In accordance with the Convention, member states must establish independent national data protection authorities to monitor and enforce legislative compliance, receive concerns from data subjects, and sanction violations (Greenleaf & Cottier, 2022). *Personal Data Protection Guidelines for Africa* compliments the Malabo Convention and includes principles like data minimization and accountability measures while clarifying the text of the original Convention (Greenleaf & Cottier, 2022).

Senegal's Policy Response

Article 43 of Senegal's Law N 2008-12 Concerning Personal Data Protection prohibits the collection of health data unless the data subject has given their consent, and health data processed by a healthcare provider is protected by professional confidentiality (Commission de Protection des Données Personnelles, 2008). Article 431-26 of the Penal Code prohibits non-consensual collection of health data and mandates that data subjects should be made aware of their right to access and the process of data transmission and storage (Commission de Protection des Données Personnelles, 2008). An offence under this section would result in the same punishment as if a medical professional had performed a treatment without informed consent (Commission de Protection des Données Personnelles, 2008).

Senegal is a leader in adopting international instruments for data protection: it was one of the first states to ratify the Malabo Convention, and one of few African states to sign Convention 108+. As a member of the Economic Community of West African States (ECOWAS), Senegal is in a position to influence other states in adopting data protection laws and support digital transformation through the *Supplementary Act on Personal Data Protection within ECOWAS* (Heng, Tsilionis, Scharff, & Wautelet, 2022; Greenleaf & Cottier, 2022). Although influenced by the Malabo and Budapest Conventions, of which Senegal acceded, Senegal's Cybercrime Law is incongruent with their legislative recommendations (Mabunda, 2025). Senegal published the

Senegalese National Cybersecurity Strategy in 2022 with goals to update its data protection and cybersecurity laws to correspond with forthcoming AI advancements (Sall, 2024).

No AI policy exists in Senegal, but the government plans to invest heavily in AI technology development as part of its 'Digital Senegal 2025' initiative (Heng, Tsilionis, Scharff, & Wautelet, 2022). Currently, Senegal mandates the use of local data to train AI models, but this is not sustainable and will erode the quality of their developing systems (Ayana, et al., 2024).

Recommendations for Successful Implementation

Existing data protection regulations must be updated before AI-based healthcare technologies can be implemented successfully. The use of AI in healthcare must be specifically addressed, not simply governed by sui generis legislation, because of the nuanced privacy considerations in the ethical collection of a patient's health data (Nyamawe, 2025).

Balance Innovation and Privacy

There is tension between data governance and technological development. AI governance will need to preserve privacy while simultaneously allowing the algorithms access to vast amounts of data (Ibeneme, et al., 2021). Regulations must be cognisant not to overly limit the collection and storage of data, which can result in biased or under representative AI models (Moreno-Sénchez, Del Ser, van Gils, & Hernesniemi, 2025). Conversely, all proposed health interventions need to be rigorously scrutinized for accountability and risk mitigation (Ibeneme, et al., 2021). Regulatory bodies have to find a balance between ethical and informed adoption while still allowing innovation to improve the capabilities of AI-based healthcare technologies. Regulatory collaboration between African governments, private actors, academics, and institutions like the World Health Organization could improve healthcare access without compromising data security (Ibeneme, et al., 2021). Drawing from existing frameworks can legitimize states in international institutions by providing a reference guiding the ethical use of AI-based healthcare technologies (David, et al., 2025). Both international and domestic regulations should include review mechanisms to adapt to evolving ethical standards (David, et al., 2025).

Human-centric Approach

Regulatory frameworks should be derived from principles founded in the human right to privacy. Interventions that respect autonomy, accountability and transparency, and informed consent will encourage trust in AI-based healthcare technology (David, et al., 2025) Trust can be built threefold: technical confidence in the accuracy of the model, regulatory trust and established enforcement mechanisms, and human confidence in the security of the models (Zahlan, Ranjan, & Hayes, 2023). Modular accuracy can be achieved with fair and unbiased algorithms (Ibeneme, et al., 2021). Training the model with diverse datasets and complying with regulatory frameworks during development can mitigate bias initially, but because they continuously evolve, it can be difficult to identify the cause of errors in AI models without built-in auditability measures (Ahadian, Xu, Liu, & Guan, 2026). Polevikov introduces ‘algorithmovigilance’, which describes the need for constant re-evaluation of algorithms to guarantee fairness and eliminate bias (2023). The lack of explainability in AI models can be improved by implementing rule-based administration for healthcare professionals to understand the model’s decision-making process, building in ethical specifications and regulations, and developing the model with interpretable machine learning algorithms (Lalwani, et al., 2024). Refining explainability and improving the digital literacy of healthcare providers and patients would make AI-based healthcare technologies easier to moderate and more transparent (Lalwani, et al., 2024). A human-centric approach to data governance grounds the above recommendations in a configuration that builds mutual trust between data subjects and AI institutions (Effoduh, Akpudo, & Kong, 2024).

International and Regional Collaboration

Beyond institutional collaboration, a global collaborative culture should be encouraged to enable transparency, fairness, and data sharing (Polevikov, 2023). Digital sovereignty should not come at the expense of data sharing: otherwise, AI models will develop bias from homogeneous datasets (Ahadian, Xu, Liu, & Guan, 2026). Balanced datasets would include representation across genders, ages, geographical regions, races, and socioeconomic statuses at a magnitude which is only possible with global cooperation (Ahadian, Xu, Liu, & Guan, 2026). Regional organisations like ECOWAS should cooperate to pool datasets and bolster infrastructures (Durokifa, 2024). It is important that in the process of importing AI systems and exporting data that networks of ‘data colonialism’ are not established (Effoduh, Akpudo, & Kong, 2024). To accomplish technological decolonization, data sharing should flow both ways where countries that provide data should benefit from access to the algorithms trained on it (Ayana, et al., 2024).

Public and Private Sector Partnerships

Since over 60% of healthcare funding in Africa comes from private actors it is important to create partnerships with the public sector to make sure that technological interventions are feasible (Dako, et al., 2025). Public involvement would situate interventions in the unique sociocultural norms and practices of the targeted community (Nyamawe, 2025). To protect against predatory private entities, it is important to strengthen domestic regulations and capacities so African states do not need to rely on extraterritorial infrastructures (Effoduh, Akpudo, & Kong, 2024). Partnering with small and medium enterprises can create more personalized solutions because of the proximity to healthcare providers and ability to address the specific needs of the community (Alami, et al., 2025). Digital interventions can improve the efficiency of health systems, but they require upfront infrastructure and workforce investments (Dako, et al., 2025). Africa has a shortage of professionals with specialized expertise in machine learning, algorithm development, and programming competencies, all of which are required to develop and maintain AI-based healthcare technologies (Durokifa, 2024). Current financial commitments are insufficient to meet the growing demand for AI technologies, ergo governments should allocate funding to domestic AI companies to expand opportunities and remove barriers to the adoption of AI-based healthcare technologies (Nyamawe, 2025).

Conclusion

Health innovations and developing technologies are crucial to improving universal access to healthcare. Although AI technologies propose transformational healthcare solutions to assist African countries, including Senegal, in meeting development goals and reducing disease burden, most states are currently lacking in infrastructure, funding, and regulation to implement them. Improper data protections leave patient’s sensitive health data vulnerable to breaches that which have serious personal consequences for patients with stigmatized diagnoses. Apprehension of the security of AI models can dissuade patients from receiving treatment. Data subjects should by awarded the right to be forgotten and limit non-consensual collection and processing of health data. States should introduce robust data protection regulations specifically for the use of AI in healthcare that prioritize accountability, transparency, informed consent, and privacy.

References

Ademuyiwa, I., & Adeniran, A. (2020). *Assessing Digitalization and Data Governance Issues in Africe: Assessing Data Protection and Privacy in Africa.* Centre for International Governance Innovation.

Ahadian, P., Xu, W., Liu, D., & Guan, Q. (2026). Ethics of trustworthy AI in healthcare: Challenges, principles, and practical pathways. *Neurocomputing*.

Alami, H., Rivard, L., Lehoux, P., Ahmed, M. A., Soubra, R., Rouquet, R., . . . Fortin, J.-P. (2025). Conflicts and complexities around intellectual property and value sharing of artificial intelligence healthcare solutions in public-private partnerships: A qualitative study. *SSM-Health Systems*.

Amini, M., Jesus, M., Sheikholeslami, D. F., Alves, P., Benam, A. H., & Hariri, F. (2023). Artificial Intelligence Ethics and Challenges in Healthcare Applications: A Comprehensive Review in the Context of the European GDPR Mandate. *Machine Learning & Knowledge Extraction*, 1023-1035.

Ayana, G., Dese, K., Nemomssa, H. D., Habtamu, B., Mellado, B., Badu, K., . . . Kong, J. D. (2024). Decolonizing global AI governance: assessment of the state of decolonized AI governance in Sub-Saharan Africa. *Royal Society Open Science*.

Ba, M., Kachallah, A. M., Kodengar, T., Gueye, K., Ngom, I., & Ouya, S. (2025). MEDCHAIN-SENEGAL: A Blockchain Solution for Medical Emergency Management. *5th International Conference on Innovative Research in Applied Science, Engineering and Technology.*

Bavli, I., Ho, A., Mahal, R., & McKeown, M. J. (2025). Ethical concerns around privacy and data security in AI health monitoring for Parkinson's disease: insights from patients, family members, and healthcare professionals. *AI & Society*, 155-165.

Charfare, R. H., Desai, A. U., Keni, N. N., Namiar, A. S., & Cherian, M. M. (2024). IoT-AI in Healthcare: A Comprehensive Survey of Current Applications and Innovations. *International Journal of Robotics and Control Systems*, 1446-1472.

Commission de Protection des Données Personnelles. (2008, January 25). Law N 2008-12 Concerning Personal Data Protection. *Laws, Regulations and Community Measures Relative to Personnal Data Protection in Senegal*. Senegal.

Dako, F., Moraes, F. Y., Doo, F., Abed, M., Anazodo, U., Patrick, L., . . . Hricak, H. (2025). Digital health and artificial intelligence innovations for oncology in sub-Saharan Africa. *Lancet Oncol*, 547-557.

David, O., Alzaidi, M. S., Ringu, V., Eltahir, M., Jungmann, F., & Jorg, T. (2025). Ethical Challenges in Big Data and AI Use for Personalized Healthcare.

Dibble, K. E., Baral, S. D., Beymer, M. R., Stahlman, S., Lyons, C. E., Olawore, O., . . . Murray, S. (2022). Stigma and healthcare access among men who have sex with men and transgender women who have sex with men in Senegal. *SAGE Open Medicine*.

Durokifa, A. A. (2024). Innovation to Impact: Implementing Artificial Intelligence (AI) Policies for Africa's Development. *Hong Kong Journal of Social Sciences*.

Dziedzic, A., Issa, J., Chaurasia, A., & Tanasiewicz, M. (2024). Artificial intelligence and health-related data: The patient's best interest and data ownership dilemma. *Journal of Engineering in Medicine*, 1-6.

Effoduh, J. O., Akpudo, U. E., & Kong, J. D. (2024). Toward a trustworthy and inclusive data governance policy for the use of artificial intelligence in Africa. *Data & Policy*.

Fidler, M. (2023). Infrastructure, Law, and Cyber Instability: An African Case Study. In R. Chesney, J. Shires, & M. Smeets, *Cyberspace and Instability.* Edinburgh University Press.

Friedland, B. A., Gottert, A., Hows, J., Baral, S. D., Sprague, L., Nyblade, L., . . . Pulerwitz, J. (2020). The People Living with HIV Stigma Index 2.0: generating critical evidence for change worldwide. *AIDS*, 5-18.

Gerke, S., Minssen, T., & Cohen, G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. *Artificial Intelligence in Healthcare*, 295-336.

Greenleaf, G., & Cottier, B. (2022). International and regional commitments in African data privacy laws: A comparative analysis. *Computer Law & Security Review*.

Heng, S., Tsilionis, K., Scharff, C., & Wautelet, Y. (2022). Understanding AI ecosystems in the Global South: The cases of Senegal and Cambodia. *International Journal of Information Management*.

Higa, H., Bedikian, S., & Costa, L. (2025, May 20). The Right to Be Forgotten Is Dead: Data Lives Forever in AI. *Tech Policy Press*.

Ibeneme, S., Okeibunor, J., Muneene, D., Husain, I., Bento, P., Gaju, C., . . . Makubalo, L. (2021). Data revolution, health status transformation and the role of artificial intelligence for health and pandemic preparedness in the African context. *BMC Proceedings.*

Ilori, T. (2020). *Data Protection in Africa and the COVID-19 Pandemic: Old Problems, New Challenges and Multistakeholder Solutions.* Association for Progressive Communications.

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*.

Kiemde, S. M., & Kora, A. D. (2020). The Challenges Facing the Development of AI in Africa. *International Conference on Advent Trends in Multidisciplinary Research and Innovation.*

Lalwani, N., Basit Ur Rahim, M. A., Anand, A., Shaik, S. P., Moghe, G. S., & Datta, D. (2024). Survey on Ethical Challenges of Implementing AI in Healthcare. *7th International Conference on Pattern Recognition and Artificial Intelligence*, (pp. 824-834). Hangzhou.

Mabunda, S. (2025). The South African and Senegalese Legislative Response to Malware-Facilitated Cybercrime. In D. Gritzalis, K.-K. R. Choo, & C. Patsakis, *Malware: Handbook of Prevention and Detection* (pp. 233-249). Springer.

Makulilo, A. B. (2024). Data privacy in Africa: Taking stock of its development after two decades. In L. A. Abdulrauf, & H. Dube, *Data privacy law in Africa: Emerging perspectives* (pp. 41-73). Pretoria: Pretoria University Law Press.

Mantelero, A. (2021). The future of data protection: Gold standard vs. global standard. *Computer Law & Security Review*.

Mohammed, S., & Malhotra, N. (2025). Ethical and regulatory challenges in machine learning-based healthcare systems: A review of implementation barriers and future directions. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*.

Moreno-Sénchez, P. A., Del Ser, J., van Gils, M., & Hernesniemi, J. (2025). A design framework for operationalizing trustworthy artificial intelligence in healthcare: Requirements, tradeoffs and challenges for its clinical adoption. *Information Fusion*.

Moulaei, K., Akhlaghpour, S., & Fatehi, F. (2025). Patient consent for the secondary use of health data in artificial intelligence (AI) models: A scoping review. *International Journal of Medical Informatics*.

Munung, N. S., Staunton, C., Mazibuko, O., Wall, P., & Wonkam, A. (2024). Data protection legislation in Africa and pathways for enhancing compliance in big data health research. *Health Research Policy and Systems*.

Ndiaye, M., Saade, R. G., & Liu, H. (2025). Understanding the impact of digitalization transition of Senegal and its implication on human health and wellbeing. *Global Transitions*, 37-55.

Ndione, A. G., Procureur, F., Senne, J.-N., Cornaglia, F., Gueye, K., Ndour, C. T., & Lépine, A. (2022). Sexuality-based stigma and access to care: intersecting perspectives between healthcare providers and men who have sex with men in HIV care centres in Senegal. *Health Policy and Planning*, 587-596.

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

Nyamawe, A. S. (2025). Is the public sector Africa's hidden force for AI-driven healthcare transformation? *Telematics and Informatics Reports*.

Odero, B., Nderitu, D., & Samuel, G. (2024). The Ubuntu Way: Ensuring Ethical AI Integration in Health Research. *Wellcome Open Research*.

Oganesian, T. D. (2020). The Right to Privacy and Data Protection in the Information Age. *Journal of Siberian Federal University: Humanities & Social Sciences*, 1576-1589.

Polevikov, S. (2023). Advancing AI in healthcare: A comprehensive review of best practices. *Clincia Chimica Acta*.

Rosen, J. G., Stone, E. M., & Mbizvo, M. T. (2023). Age-of-consent requirements and adolescent HIV testing in low-and middle-income countries: multinational insights from 51 population-based surveys. *International Journal of STD & AIDS*, 168-174.

Salami, E. (2024). The ascent of artificial intelligence in Africa: Bridging innovation and data protection. In L. Abdulrauf, & H. Dube, *Data privacy law in Africa: Emerging perspectives.*

Sall, C. (2024). Analysis of cyber incidents in Senegal from 2005-2023. *The African Journal of Information and Communication*, 1-19.

Slokenberga, S. (2020). Biobanking and data transfer between the EU and Cape Verde, Mauritius, Morocco, Senegal, and Tunisia: adequacy considerations and Convention 108. *International Data Privacy Law*, 132-145.

Soulé, F. (2024). *Digital Sovereignty in Africa: Moving beyond Local Data Ownership.* Centre for International Governance Innovation.

Turinici, M., Petcu, I., & Paraschiv, C. (2025). AI-driven Health Data Governance: The Risks and Challenges of Datafication. *Romanian Cyber Security Journal*.

World Health Organization. (2023). *Regulatory considerations on artificial intelligence for health.* Geneva.

Yener, R., Chen, G.-H., Gumusel, E., & Bashir, M. (2025). Can I Trust This Chatbot? Assessing User Privacy in AI-Healthcare Chatbot Applications. *Difficult Conversations: The Role of Information Science in the Age of Human-Centred Artificial Intelligence* (pp. 809-820). Washington: 88th Annual Meeting of the Association for Information Science and Technology.

Zahlan, A., Ranjan, R. P., & Hayes, D. (2023). Artificial intelligence innovation in healthcare: Literature review, exploratory analysis, and future research. *Technology in Society*.

Appendix A

Completed Search Strategy Chart

Search Term: "AI health" AND "Senegal" AND "data protection"			
Database	**Total # of Articles**	**Articles**	**Date**
Omni	0		November 6, 2025
Google Scholar	24	Towards an Inclusive Data Governance Policy for the Use of Artificial Intelligence in Africa	
		Data revolution, health status transformation and the role of artificial intelligence for health and pandemic preparedness in the African context	
		Artificial Intelligence and Cancer Care in Africa	
		A Qualitative Inquiry Exploring Perceptions of Artificial Intelligence to Improve Outcomes in Maternal, Sexual and Reproductive Health in Sub-Saharan Africa	
		The Ubuntu Way: Ensuring Ethical AI Integration in Health Research	
		The Challenges Facing the Development of AI in Africa	
PubMed	0		
Science Direct	1	Artificial Intelligence and Cancer Care in Africa	
JSTOR	0		

Search Term: “AI health” AND “data protection”			
Database	**Total # of Articles**	**Articles**	**Date**
Omni	6	Ethical concerns around privacy and data security in AI health monitoring for Parkinson’s disease: insights from patients, family members, and healthcare professionals	November 7, 2025
		Artificial Intelligence Ethics and Challenges in Healthcare Applications: A Comprehensive Review in the Context of the European GDPR Mandate	
Google Scholar	1,340	Protecting Sensitive Health Data in AI-based Research and Development	
		Artificial intelligence and health-related data: The patient’s best interest and data ownership dilemma	
		Implications of Artificial Intelligence on Health Data Privacy and Confidentiality	
		Data Privacy and Security Concerns in AI-Driven Healthcare	
		Patient consent for the secondary use of health fata in artificial intelligence (AI) models: A scoping review	
		Regulatory considerations on artificial intelligence for health	
		AI-driven Health Data Governance: The Risks and Challenges of Datafication	
		Can I Trust This Chatbot? Assessing User Privacy in AI-Healthcare Chatbot Applications	

		Ethical Challenges in Big Data and AI Use for Personalized Healthcare	
		Mapping the Legal Landscape: A Comparative Study of Regulatory Frameworks Governing AI Health Applications	
PubMed	4	The Ubuntu Way: Ensuring Ethical AI Integration in Health Research	
Science Direct	101	Ethical and regulatory challenges in machine learning-based healthcare systems: A review of implementation barriers in future directions	
		Ethical and legal challenges of artificial intelligence-driven healthcare	
		Patient consent for the secondary use of health data in artificial intelligence (AI) models: a scoping review	
JSTOR	8	*no relevant articles*	
Notes Google Scholar: search stopped after page 5, results were repetitive and compiled articles were comprehensive.			

Search Term: "data collection" AND "AI healthcare"

Database	**Total # of Articles**	**Articles**	**Date**
Omni	8	Assuring assistance to healthcare and medicine: Internet of Things, Artificial Intelligence, and Artificial Intelligence of Things	November 7, 2025
		Artificial intelligence innovation in healthcare: Literature review, exploratory analysis, and future research	
Google Scholar	3,150	IoT-AI in Healthcare: A Comprehensive Survey of Current Applications and Innovations	
		Advancing AI in healthcare: A comprehensive review of best practices	
		Survey on Ethical Challenges of Implementing AI in Healthcare	
PubMed	2	Assuring assistance to healthcare and medicine: Internet of Things, Artificial Intelligence, and Artificial Intelligence of Things	
Science Direct	221	Artificial intelligence innovation in healthcare: Literature review, exploratory analysis, and future research	
		Ethics of trustworthy AI in healthcare: Challenges, principles, and practical pathways	
		Chapter 1 – Bridging data and diagnostics: an introduction to artificial intelligence-driven healthcare optimization	
		A design framework for operationalizing trustworthy artificial intelligence in healthcare: Requirements, tradeoffs and challenges for its clinical adoption	
		Conflicts and complexities around intellectual property and value sharing of artificial intelligence healthcare solutions in public-private partnerships: A qualitative study	
		Privacy-preserving artificial intelligence in healthcare: Techniques and applications	
JSTOR	4	*no relevant articles*	
Notes Google Scholar: the search term was too broad and many results were irrelevant. Relevant articles were repetitive. Science Direct: the search term was too broad and many results were irrelevant.			

Search Term: “data protection” AND “Senegal”			
Database	**Total # of Articles**	**Articles**	**Date**
Omni	23	Biobanking and data transfer between the EU and Cape Verde, Mauritius, Morocco, Senegal, and Tunisia: adequacy considerations and Convention 108	November 9, 2025
Google Scholar	4,420	Data protection in Africa and the Covid-19 pandemic: Old problems, new challenges and multistakeholder solutions	
		Analyses of selected legal issues related to personal data security and the inter-relationship between personal data protection law in Africa and Europe	
		Data protection legislation in Africa and pathways for enhancing compliance in big data health research	
		Analysis of cyber incidents in Senegal from 2005 to 2023	
		DATA PRIVACY IN AFRICA	
		Biobanking in Sub-Saharan Africa: A Review of Data Protection Frameworks	
		Data protection in Africa: Slowly but Surely	
		Big Data, Internet Privacy and the Vulnerabilities of the African Regulatory Landscape	
		MEDCHAIN-SENEGAL: a blockchain solution for medical emergency management	
		The South African and Senegalese Legislative Response to Malware-Facilitated Cybercrime	
		Proposal for an IoT-based e-health model in developing countries: case of Senegal	
PubMed	2	Decolonizing global AI governance: assessment of the state of decolonized AI governance in Sub-Saharan Africa	
Science Direct	106	Understanding the impact of digitalization transition of Senegal and its implication on human health and wellbeing	
		The future of data protection: Gold standard vs. global standard	
		Understanding AI ecosystems in the Global South: the cases of Senegal and Cambodia	
		International and regional commitments in African data privacy laws: A comparative analysis	
		Application of medical artificial intelligence technology in sub-Saharan Africa: prospects for medical laboratories	
		Mobile health applications for disease screening and treatment support in low-and middle-income countries: a narrative review	
JSTOR	88	Assessing Data Protection and Privacy in Africa	
		Data Localization: A “Tax” on the Poor	
		AI Innovation Concentration and the Governance Challenge	
		Infrastructure, Law, and Cyber Instability: An African Case Study	
Notes Google Scholar: search was stopped at page 5, results were irrelevant.			

Search Term: “data protection” AND “enforcement” AND “Senegal”			
Database	**Total # of Articles**	**Articles**	**Date**
Omni	1	*no relevant articles*	November 9, 2025
Google Scholar	1,550	Africa’s Data Privacy Puzzle: Data Privacy Laws and Compliance in Selected African Countries	
		An assessment of the enforcement mechanisms in African data protection laws	
		Digital Sovereignty in Africa: Moving Beyond Local Data Ownership	
		Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights	
PubMed	0		
Science Direct	24	Artificial Intelligence And Cancer Care in Africa	
		Digital health and artificial intelligence innovations for oncology in sub-Saharan Africa	
		Is the public sector Africa’s hidden force for AI-driven healthcare transformation?	
JSTOR	44	*no relevant articles*	

Search Term: “data collection” AND “Senegal” AND “HIV” AND “data protection”			
Database	**Total # of Articles**	**Articles**	**Date**
Omni	0		November 9, 2025
Google Scholar	381	Ethical, legal, and sociocultural issues in the use of mobile technologies and call detail records data for public health in the East African region	
		Artificial intelligence for public health surveillance in Africa: applications and opportunities	
		Achieving HIV treatment targets in the era of digital health: the promises and challenges of mHealth	
		The Right to Privacy and Data Protection in the Information Age	
		The Ascent of Artificial Intelligence in Africa: Bridging Innovation and Data Protection	
		Addressing ethical issues for health and demographic surveillance systems in sub-Saharan Africa	
		Health Data Digitalization in Africa	
PubMed	0		
Science Direct	17	*no relevant articles*	
JSTOR	6	*no relevant articles*	
Notes Google Scholar: search stopped at page 5, results were irrelevant.			

Search Term: “AU Convention on Cybersecurity” AND “Senegal”			
Database	**Total # of Articles**	**Articles**	**Date**
Omni	0		

Google Scholar	27	Analysis of cyber incidents in Senegal from 2005 to 2023	November 9, 2025
		Regional cybersecurity approaches in Africa and Latin America	
		Analyses of selected legal issues related to personal data security and the inter-relationship between personal data protection law in Africa and Europe	
		African governments and the influence of corruption on the proliferation of cybercrime in Africa: wherein lies the rule of law?	
		Regional data protection policy and artificial intelligence	
		Algorithms of Oppression? AU's cybersecurity policy and its enforcement in Africa	
PubMed	0		
Science Direct	0		
JSTOR	0		
Notes Google Scholar: results were relevant but became repetitive.			

Search Term: "AU Convention on Cybersecurity" AND "Senegal" AND "health"			
Database	**Total # of Articles**	**Articles**	**Date**
Omni	0		November 9, 2025
Google Scholar	16	Innovation to Impact: Implementing Artificial Intelligence (AI) Policies for Africa's Development	
		Protecting the Patient's Data in the 21st Century Healthcare Industry: Is the African Continent Ready for the Digital Space?	
		Toward a trustworthy and inclusive data governance policy for the use of artificial intelligence in Africa	
		Data Protection Legal Regime and Data Governance in Africa: An Overview	
PubMed	0		
Science Direct	0		
JSTOR	0		

Search Term: "data collection" AND "Senegal" AND "HIV" AND "stigma"			
Database	**Total # of Articles**	**Articles**	**Date**
Omni	3	*no relevant articles*	November 9, 2025
Google Scholar	2,870	Sexuality-based stigma and access to care: intersecting perspectives between healthcare providers and men who have sex with men in HIV care centres in Senegal	
		The People Living with HIV Stigma Index 2.0: generating critical evidence for change worldwide	
		Disclosure of same-sex practices and experiences of healthcare stigma among cisgender men who have sex with men in five sub-Saharan African countries	
PubMed	3	Stigma and healthcare access among men who have sex with men and transgender women who have sex with men in Senegal	

Science Direct	83	HIV stigma beliefs and unprotected sex among teenagers and young adults in sub-Saharan Africa: the moderating role of mass media exposure	
		Nothing but the truth: Consistency and efficiency of the list experiment method for the measurement of sensitive health behaviours	
		Barriers to post exposure prophylaxis use among men who have sex with men in sub-Saharan Africa: An online cross-sectional survey	
JSTOR	51	*no relevant articles*	
Notes Google Scholar: search stopped at page 4, results became irrelevant. Science Direct: search stopped at page 2, results became irrelevant.			

Manual Search Term: "health" AND "age of consent" AND "Senegal"			
Database	**Total # of Articles**	**Articles**	**Date**
Google Scholar	292	Legal Age of Consent for HIV Testing Among Adolescents in Sub Saharan Africa, A Systematic Review	November 25, 2025
		Age-of-consent requirements and adolescent HIV testing in low-and middle-income countries: multinational insights from 51 population-based surveys	

Appendix B

Article Inclusion Process

TOTAL COLLECTED ARTICLES BY TITLE:	**87**
# of Articles Removed Because of Duplicates:	6
TOTAL COLLECTED ARTICLES WITH DUPLICATES REMOVED:	**81**
# of Articles Removed Because of Irrelevant Abstracts:	11
TOTAL ARTICLES RELEVANT FROM ABSTRACT:	**70**
# of Articles Removed Because of Irrelevance After Complete Review:	22
TOTAL ARTICLES RELEVENT IN ENTIRETY:	**48**
Total # of Articles Removed	39

INITIAL SEARCH OF ARTICLES	
Towards an Inclusive Data Governance Policy for the Use of Artificial Intelligence in Africa	X
Data revolution, health status transformation and the role of artificial intelligence for health and pandemic preparedness in the African context	X
Artificial Intelligence and Cancer Care in Africa	N
A Qualitative Inquiry Exploring Perceptions of Artificial Intelligence to Improve Outcomes in Maternal, Sexual and Reproductive Health in Sub-Saharan Africa	X
The Ubuntu Way: Ensuring Ethical AI Integration in Health Research	N
The Challenges Facing the Development of AI in Africa	X
Ethical concerns around privacy and data security in AI health monitoring for Parkinson's disease: insights from patients, family members, and healthcare professionals	X
Artificial Intelligence Ethics and Challenges in Healthcare Applications: A Comprehensive Review in the Context of the European GDPR Mandate	X
Protecting Sensitive Health Data in AI-based Research and Development	X
Artificial intelligence and health-related data: The patient's best interest and data ownership dilemma	X
Implications of Artificial Intelligence on Health Data Privacy and Confidentiality	X
Data Privacy and Security Concerns in AI-Driven Healthcare	X
Patient consent for the secondary use of health data in artificial intelligence (AI) models: A scoping review	X
Regulatory considerations on artificial intelligence for health	X
AI-driven Health Data Governance: The Risks and Challenges of Datafication	X
Can I Trust This Chatbot? Assessing User Privacy in AI-Healthcare Chatbot Applications	X
Ethical Challenges in Big Data and AI Use for Personalized Healthcare	X
Mapping the Legal Landscape: A Comparative Study of Regulatory Frameworks Governing AI Health Applications	X
The Ubuntu Way: Ensuring Ethical AI Integration in Health Research	N
Ethical and regulatory challenges in machine learning-based healthcare systems: A review of implementation barriers in future directions	X
Ethical and legal challenges of artificial intelligence-driven healthcare	X
Assuring assistance to healthcare and medicine: Internet of Things, Artificial Intelligence, and Artificial Intelligence of Things	N
Artificial intelligence innovation in healthcare: Literature review, exploratory analysis, and future research	N
IoT-AI in Healthcare: A Comprehensive Survey of Current Applications and Innovations	X
Advancing AI in healthcare: A comprehensive review of best practices	X
Survey on Ethical Challenges of Implementing AI in Healthcare	X
Assuring assistance to healthcare and medicine: Internet of Things, Artificial Intelligence, and Artificial Intelligence of Things	N
Artificial intelligence innovation in healthcare: Literature review, exploratory analysis, and future research	N
Ethics of trustworthy AI in healthcare: Challenges, principles, and practical pathways	X

ARTICLES WITH DUPLICATES REMOVED	
Towards an Inclusive Data Governance Policy for the Use of Artificial Intelligence in Africa	X
Data revolution, health status transformation and the role of artificial intelligence for health and pandemic preparedness in the African context	X
Artificial Intelligence and Cancer Care in Africa	X
A Qualitative Inquiry Exploring Perceptions of Artificial Intelligence to Improve Outcomes in Maternal, Sexual and Reproductive Health in Sub-Saharan Africa	X
The Ubuntu Way: Ensuring Ethical AI Integration in Health Research	X
The Challenges Facing the Development of AI in Africa	X
Ethical concerns around privacy and data security in AI health monitoring for Parkinson's disease: insights from patients, family members, and healthcare professionals	X
Artificial Intelligence Ethics and Challenges in Healthcare Applications: A Comprehensive Review in the Context of the European GDPR Mandate	X
Protecting Sensitive Health Data in AI-based Research and Development	N
Artificial intelligence and health-related data: The patient's best interest and data ownership dilemma	X
Implications of Artificial Intelligence on Health Data Privacy and Confidentiality	X
Data Privacy and Security Concerns in AI-Driven Healthcare	X
Patient consent for the secondary use of health data in artificial intelligence (AI) models: A scoping review	X
Regulatory considerations on artificial intelligence for health	X
AI-driven Health Data Governance: The Risks and Challenges of Datafication	X
Can I Trust This Chatbot? Assessing User Privacy in AI-Healthcare Chatbot Applications	X
Ethical Challenges in Big Data and AI Use for Personalized Healthcare	X
Mapping the Legal Landscape: A Comparative Study of Regulatory Frameworks Governing AI Health Applications	N
Ethical and regulatory challenges in machine learning-based healthcare systems: A review of implementation barriers in future directions	X
Ethical and legal challenges of artificial intelligence-driven healthcare	X
Artificial intelligence innovation in healthcare: Literature review, exploratory analysis, and future research	X
IoT-AI in Healthcare: A Comprehensive Survey of Current Applications and Innovations	X
Advancing AI in healthcare: A comprehensive review of best practices	X
Survey on Ethical Challenges of Implementing AI in Healthcare	X
Assuring assistance to healthcare and medicine: Internet of Things, Artificial Intelligence, and Artificial Intelligence of Things	X
Ethics of trustworthy AI in healthcare: Challenges, principles, and practical pathways	X
Chapter 1 – Bridging data and diagnostics: an introduction to artificial intelligence-driven healthcare optimization	X
A design framework for operationalizing trustworthy artificial intelligence in healthcare: Requirements, tradeoffs and challenges for its clinical adoption	X
Conflicts and complexities around intellectual property and value sharing of artificial intelligence healthcare solutions in public-private partnerships: A qualitative study	X

ARTICLES RELEVANT FROM ABSTRACT	
Towards an Inclusive Data Governance Policy for the Use of Artificial Intelligence in Africa	X
Data revolution, health status transformation and the role of artificial intelligence for health and pandemic preparedness in the African context	X
Artificial Intelligence and Cancer Care in Africa	N
A Qualitative Inquiry Exploring Perceptions of Artificial Intelligence to Improve Outcomes in Maternal, Sexual and Reproductive Health in Sub-Saharan Africa	N
The Ubuntu Way: Ensuring Ethical AI Integration in Health Research	X
The Challenges Facing the Development of AI in Africa	X
Ethical concerns around privacy and data security in AI health monitoring for Parkinson's disease: insights from patients, family members, and healthcare professionals	X
Artificial Intelligence Ethics and Challenges in Healthcare Applications: A Comprehensive Review in the Context of the European GDPR Mandate	X
Artificial intelligence and health-related data: The patient's best interest and data ownership dilemma	X
Implications of Artificial Intelligence on Health Data Privacy and Confidentiality	X
Data Privacy and Security Concerns in AI-Driven Healthcare	X
Patient consent for the secondary use of health data in artificial intelligence (AI) models: A scoping review	X
Regulatory considerations on artificial intelligence for health	X
AI-driven Health Data Governance: The Risks and Challenges of Datafication	X
Can I Trust This Chatbot? Assessing User Privacy in AI-Healthcare Chatbot Applications	X
Ethical Challenges in Big Data and AI Use for Personalized Healthcare	X
Ethical and regulatory challenges in machine learning-based healthcare systems: A review of implementation barriers in future directions	X
Ethical and legal challenges of artificial intelligence-driven healthcare	X
Artificial intelligence innovation in healthcare: Literature review, exploratory analysis, and future research	X
IoT-AI in Healthcare: A Comprehensive Survey of Current Applications and Innovations	X
Advancing AI in healthcare: A comprehensive review of best practices	X
Survey on Ethical Challenges of Implementing AI in Healthcare	X
Assuring assistance to healthcare and medicine: Internet of Things, Artificial Intelligence, and Artificial Intelligence of Things	N
Ethics of trustworthy AI in healthcare: Challenges, principles, and practical pathways	X
Chapter 1 – Bridging data and diagnostics: an introduction to artificial intelligence-driven healthcare optimization	N
A design framework for operationalizing trustworthy artificial intelligence in healthcare: Requirements, tradeoffs and challenges for its clinical adoption	X
Conflicts and complexities around intellectual property and value sharing of artificial intelligence healthcare solutions in public-private partnerships: A qualitative study	X
Privacy-preserving artificial intelligence in healthcare: Techniques and applications	X
Biobanking and data transfer between the EU and Cape Verde, Mauritius, Morocco, Senegal, and Tunisia: adequacy considerations and Convention 108	X

ARTICLES TO BE INCLUDED IN LIT REVIEW
Towards an Inclusive Data Governance Policy for the Use of Artificial Intelligence in Africa
Data revolution, health status transformation and the role of artificial intelligence for health and pandemic preparedness in the African context
The Ubuntu Way: Ensuring Ethical AI Integration in Health Research
The Challenges Facing the Development of AI in Africa
Ethical concerns around privacy and data security in AI health monitoring for Parkinson's disease: insights from patients, family members, and healthcare professionals
Artificial Intelligence Ethics and Challenges in Healthcare Applications: A Comprehensive Review in the Context of the European GDPR Mandate
Artificial intelligence and health-related data: The patient's best interest and data ownership dilemma
Implications of Artificial Intelligence on Health Data Privacy and Confidentiality
Data Privacy and Security Concerns in AI-Driven Healthcare
Patient consent for the secondary use of health data in artificial intelligence (AI) models: A scoping review
Regulatory considerations on artificial intelligence for health
AI-driven Health Data Governance: The Risks and Challenges of Datafication
Can I Trust This Chatbot? Assessing User Privacy in AI-Healthcare Chatbot Applications
Ethical Challenges in Big Data and AI Use for Personalized Healthcare
Ethical and regulatory challenges in machine learning-based healthcare systems: A review of implementation barriers in future directions
Ethical and legal challenges of artificial intelligence-driven healthcare
Artificial intelligence innovation in healthcare: Literature review, exploratory analysis, and future research
IoT-AI in Healthcare: A Comprehensive Survey of Current Applications and Innovations
Advancing AI in healthcare: A comprehensive review of best practices
Survey on Ethical Challenges of Implementing AI in Healthcare
Ethics of trustworthy AI in healthcare: Challenges, principles, and practical pathways
A design framework for operationalizing trustworthy artificial intelligence in healthcare: Requirements, tradeoffs and challenges for its clinical adoption
Conflicts and complexities around intellectual property and value sharing of artificial intelligence healthcare solutions in public-private partnerships: A qualitative study
Privacy-preserving artificial intelligence in healthcare: Techniques and applications
Biobanking and data transfer between the EU and Cape Verde, Mauritius, Morocco, Senegal, and Tunisia: adequacy considerations and Convention 108
Data protection in Africa and the Covid-19 pandemic: Old problems, new challenges and multistakeholder solutions
Data protection legislation in Africa and pathways for enhancing compliance in big data health research
Analysis of cyber incidents in Senegal from 2005 to 2023
Data Privacy in Africa: Taking stock of its development after two decades

Chapter 1 – Bridging data and diagnostics: an introduction to artificial intelligence-driven healthcare optimization	X
A design framework for operationalizing trustworthy artificial intelligence in healthcare: Requirements, tradeoffs and challenges for its clinical adoption	X
Conflicts and complexities around intellectual property and value sharing of artificial intelligence healthcare solutions in public-private partnerships: A qualitative study	X
Privacy-preserving artificial intelligence in healthcare: Techniques and applications	X
Biobanking and data transfer between the EU and Cape Verde, Mauritius, Morocco, Senegal, and Tunisia: adequacy considerations and Convention 108	X
Data protection in Africa and the Covid-19 pandemic: Old problems, new challenges and multistakeholder solutions	X
Analyses of selected legal issues related to personal data security and the inter-relationship between personal data protection law in Africa and Europe	N
Data protection legislation in Africa and pathways for enhancing compliance in big data health research	X
Analysis of cyber incidents in Senegal from 2005 to 2023	N
Data Privacy in Africa: Taking stock of its development after two decades	X
Biobanking in Sub-Saharan Africa: A Review of Data Protection Frameworks	X
Data protection in Africa: Slowly but Surely	X
Big Data, Internet Privacy and the Vulnerabilities of the African Regulatory Landscape	X
MEDCHAIN-SENEGAL: a blockchain solution for medical emergency management	X
The South African and Senegalese Legislative Response to Malware-Facilitated Cybercrime	X
Decolonizing global AI governance: assessment of the state of decolonized AI governance in Sub-Saharan Africa	X
Understanding the impact of digitalization transition of Senegal and its implication on human health and wellbeing	X
The future of data protection: Gold standard vs. global standard	X
Understanding AI ecosystems in the Global South: the cases of Senegal and Cambodia	X
International and regional commitments in African data privacy laws: A comparative analysis	X
Application of medical artificial intelligence technology in sub-Saharan Africa: prospects for medical laboratories	X
Mobile health applications for disease screening and treatment support in low-and middle-income countries: a narrative review	X
Assessing Data Protection and Privacy in Africa	X
Data Localization: A “Tax” on the Poor	X
AI Innovation Concentration and the Governance Challenge	X
Infrastructure, Law, and Cyber Instability: An African Case Study	X
Artificial Intelligence And Cancer Care in Africa	N
Digital health and artificial intelligence innovations for oncology in sub-Saharan Africa	X
Is the public sector Africa’s hidden force for AI-driven healthcare transformation?	X
Ethical, legal, and sociocultural issues in the use of mobile technologies and call detail records data for public health in the East African region	X

Privacy-preserving artificial intelligence in healthcare: Techniques and applications	X
Biobanking and data transfer between the EU and Cape Verde, Mauritius, Morocco, Senegal, and Tunisia: adequacy considerations and Convention 108	X
Data protection in Africa and the Covid-19 pandemic: Old problems, new challenges and multistakeholder solutions	X
Analyses of selected legal issues related to personal data security and the inter-relationship between personal data protection law in Africa and Europe	N
Data protection legislation in Africa and pathways for enhancing compliance in big data health research	X
Analysis of cyber incidents in Senegal from 2005 to 2023	X
Data Privacy in Africa: Taking stock of its development after two decades	X
Biobanking in Sub-Saharan Africa: A Review of Data Protection Frameworks	X
Data protection in Africa: Slowly but Surely	N
Big Data, Internet Privacy and the Vulnerabilities of the African Regulatory Landscape	N
MEDCHAIN-SENEGAL: a blockchain solution for medical emergency management	X
Chapter 10 - The South African and Senegalese Legislative Response to Malware-Facilitated Cybercrime	X
Decolonizing global AI governance: assessment of the state of decolonized AI governance in Sub-Saharan Africa	X
Understanding the impact of digitalization transition of Senegal and its implication on human health and wellbeing	X
The future of data protection: Gold standard vs. global standard	X
Understanding AI ecosystems in the Global South: the cases of Senegal and Cambodia	X
International and regional commitments in African data privacy laws: A comparative analysis	X
Application of medical artificial intelligence technology in sub-Saharan Africa: prospects for medical laboratories	X
Mobile health applications for disease screening and treatment support in low-and middle-income countries: a narrative review	X
Assessing Data Protection and Privacy in Africa	X
Data Localization: A “Tax” on the Poor	X
AI Innovation Concentration and the Governance Challenge	X
Infrastructure, Law, and Cyber Instability: An African Case Study	X
Digital health and artificial intelligence innovations for oncology in sub-Saharan Africa	X
Is the public sector Africa’s hidden force for AI-driven healthcare transformation?	X
Ethical, legal, and sociocultural issues in the use of mobile technologies and call detail records data for public health in the East African region	X
Artificial intelligence for public health surveillance in Africa: applications and opportunities	X
Achieving HIV treatment targets in the era of digital health: the promises and challenges of mHealth	N
The Right to Privacy and Data Protection in the Information Age	X
The Ascent of Artificial Intelligence in Africa: Bridging Innovation and Data Protection	X

Data protection in Africa and the Covid-19 pandemic: Old problems, new challenges and multistakeholder solutions	X
Data protection legislation in Africa and pathways for enhancing compliance in big data health research	X
Analysis of cyber incidents in Senegal from 2005 to 2023	X
Data Privacy in Africa: Taking stock of its development after two decades	X
Biobanking in Sub-Saharan Africa: A Review of Data Protection Frameworks	N
MEDCHAIN-SENEGAL: a blockchain solution for medical emergency management	X
Chapter 10 - The South African and Senegalese Legislative Response to Malware-Facilitated Cybercrime	X
Decolonizing global AI governance: assessment of the state of decolonized AI governance in Sub-Saharan Africa	X
Understanding the impact of digitalization transition of Senegal and its implication on human health and wellbeing	X
The future of data protection: Gold standard vs. global standard	X
Understanding AI ecosystems in the Global South: the cases of Senegal and Cambodia	X
International and regional commitments in African data privacy laws: A comparative analysis	X
Application of medical artificial intelligence technology in sub-Saharan Africa: prospects for medical laboratories	N
Mobile health applications for disease screening and treatment support in low-and middle-income countries: a narrative review	N
Assessing Data Protection and Privacy in Africa	X
Data Localization: A “Tax” on the Poor	N
AI Innovation Concentration and the Governance Challenge	N
Infrastructure, Law, and Cyber Instability: An African Case Study	X
Digital health and artificial intelligence innovations for oncology in sub-Saharan Africa	X
Is the public sector Africa’s hidden force for AI-driven healthcare transformation?	X
Ethical, legal, and sociocultural issues in the use of mobile technologies and call detail records data for public health in the East African region	N
Artificial intelligence for public health surveillance in Africa: applications and opportunities	N
The Right to Privacy and Data Protection in the Information Age	X
The Ascent of Artificial Intelligence in Africa: Bridging Innovation and Data Protection	X
Regional cybersecurity approaches in Africa and Latin America	N
African governments and the influence of corruption on the proliferation of cybercrime in Africa: wherein lies the rule of law?	N
Innovation to Impact: Implementing Artificial Intelligence (AI) Policies for Africa’s Development	X
Sexuality-based stigma and access to care: intersecting perspectives between healthcare providers and men who have sex with men in HIV care centres in Senegal	X
The People Living with HIV Stigma Index 2.0: generating critical evidence for change worldwide	X
Disclosure of same-sex practices and experiences of healthcare stigma among cisgender men who have sex with men in five sub-Saharan African countries	N

MEDCHAIN-SENEGAL: a blockchain solution for medical emergency management
Chapter 10 - The South African and Senegalese Legislative Response to Malware-Facilitated Cybercrime
Decolonizing global AI governance: assessment of the state of decolonized AI governance in Sub-Saharan Africa
Understanding the impact of digitalization transition of Senegal and its implication on human health and wellbeing
The future of data protection: Gold standard vs. global standard
Understanding AI ecosystems in the Global South: the cases of Senegal and Cambodia
International and regional commitments in African data privacy laws: A comparative analysis
Assessing Data Protection and Privacy in Africa
Infrastructure, Law, and Cyber Instability: An African Case Study
Digital health and artificial intelligence innovations for oncology in sub-Saharan Africa
Is the public sector Africa’s hidden force for AI-driven healthcare transformation?
The Right to Privacy and Data Protection in the Information Age
The Ascent of Artificial Intelligence in Africa: Bridging Innovation and Data Protection
Innovation to Impact: Implementing Artificial Intelligence (AI) Policies for Africa’s Development
Sexuality-based stigma and access to care: intersecting perspectives between healthcare providers and men who have sex with men in HIV care centres in Senegal
The People Living with HIV Stigma Index 2.0: generating critical evidence for change worldwide
Stigma and healthcare access among men who have sex with men and transgender women who have sex with men in Senegal
Toward a trustworthy and inclusive data governance policy for the use of artificial intelligence in Africa
Digital Sovereignty in Africa: Moving Beyond Local Data Ownership
Protecting the Patient's Data in the 21st Century Healthcare Industry: Is the African Continent Ready for the Digital Space?

Artificial intelligence for public health surveillance in Africa: applications and opportunities	X
Achieving HIV treatment targets in the era of digital health: the promises and challenges of mHealth	X
The Right to Privacy and Data Protection in the Information Age	X
The Ascent of Artificial Intelligence in Africa: Bridging Innovation and Data Protection	X
Addressing ethical issues for health and demographic surveillance systems in sub-Saharan Africa	X
Analysis of cyber incidents in Senegal from 2005 to 2023	N
Regional cybersecurity approaches in Africa and Latin America	X
Analyses of selected legal issues related to personal data security and the inter-relationship between personal data protection law in Africa and Europe	N
African governments and the influence of corruption on the proliferation of cybercrime in Africa: wherein lies the rule of law?	X
Regional data protection policy and artificial intelligence	X
Innovation to Impact: Implementing Artificial Intelligence (AI) Policies for Africa's Development	X
Sexuality-based stigma and access to care: intersecting perspectives between healthcare providers and men who have sex with men in HIV care centres in Senegal	X
The People Living with HIV Stigma Index 2.0: generating critical evidence for change worldwide	X
Disclosure of same-sex practices and experiences of healthcare stigma among cisgender men who have sex with men in five sub-Saharan African countries	X
Stigma and healthcare access among men who have sex with men and transgender women who have sex with men in Senegal	X
HIV stigma beliefs and unprotected sex among teenagers and young adults in sub-Saharan Africa: the moderating role of mass media exposure	X
Nothing but the truth: Consistency and efficiency of the list experiment method for the measurement of sensitive health behaviours	X
Barriers to post exposure prophylaxis use among men who have sex with men in sub-Saharan Africa: An online cross-sectional survey	X
Toward a trustworthy and inclusive data governance policy for the use of artificial intelligence in Africa	X
Data Protection Legal Regime and Data Governance in Africa: An Overview	X
Algorithms of Oppression? AU's cybersecurity policy and its enforcement in Africa	X
Health Data Digitalization in Africa	X
Africa's Data Privacy Puzzle: Data Privacy Laws and Compliance in Selected African Countries	X
An assessment of the enforcement mechanisms in African data protection laws	X
Digital Sovereignty in Africa: Moving Beyond Local Data Ownership	X
Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights	X
Proposal for an IoT-based e-health model in developing countries: case of Senegal	X
Protecting the Patient's Data in the 21st Century Healthcare Industry: Is the African Continent Ready for the Digital Space?	X

Addressing ethical issues for health and demographic surveillance systems in sub-Saharan Africa	N
Regional cybersecurity approaches in Africa and Latin America	X
African governments and the influence of corruption on the proliferation of cybercrime in Africa: wherein lies the rule of law?	X
Regional data protection policy and artificial intelligence	N
Innovation to Impact: Implementing Artificial Intelligence (AI) Policies for Africa's Development	X
Sexuality-based stigma and access to care: intersecting perspectives between healthcare providers and men who have sex with men in HIV care centres in Senegal	X
The People Living with HIV Stigma Index 2.0: generating critical evidence for change worldwide	X
Disclosure of same-sex practices and experiences of healthcare stigma among cisgender men who have sex with men in five sub-Saharan African countries	X
Stigma and healthcare access among men who have sex with men and transgender women who have sex with men in Senegal	X
HIV stigma beliefs and unprotected sex among teenagers and young adults in sub-Saharan Africa: the moderating role of mass media exposure	N
Nothing but the truth: Consistency and efficiency of the list experiment method for the measurement of sensitive health behaviours	X
Barriers to post exposure prophylaxis use among men who have sex with men in sub-Saharan Africa: An online cross-sectional survey	N
Toward a trustworthy and inclusive data governance policy for the use of artificial intelligence in Africa	X
Data Protection Legal Regime and Data Governance in Africa: An Overview	X
Algorithms of Oppression? AU's cybersecurity policy and its enforcement in Africa	X
Health Data Digitalization in Africa	X
Africa's Data Privacy Puzzle: Data Privacy Laws and Compliance in Selected African Countries	X
An assessment of the enforcement mechanisms in African data protection laws	X
Digital Sovereignty in Africa: Moving Beyond Local Data Ownership	X
Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights	N
Proposal for an IoT-based e-health model in developing countries: case of Senegal	X
Protecting the Patient's Data in the 21st Century Healthcare Industry: Is the African Continent Ready for the Digital Space?	X

Stigma and healthcare access among men who have sex with men and transgender women who have sex with men in Senegal	X
Nothing but the truth: Consistency and efficiency of the list experiment method for the measurement of sensitive health behaviours	N
Toward a trustworthy and inclusive data governance policy for the use of artificial intelligence in Africa	X
Data Protection Legal Regime and Data Governance in Africa: An Overview	N
Algorithms of Oppression? AU's cybersecurity policy and its enforcement in Africa	N
Health Data Digitalization in Africa	N
Africa's Data Privacy Puzzle: Data Privacy Laws and Compliance in Selected African Countries	N
An assessment of the enforcement mechanisms in African data protection laws	N
Digital Sovereignty in Africa: Moving Beyond Local Data Ownership	X
Proposal for an IoT-based e-health model in developing countries: case of Senegal	N
Protecting the Patient's Data in the 21st Century Healthcare Industry: Is the African Continent Ready for the Digital Space?	X