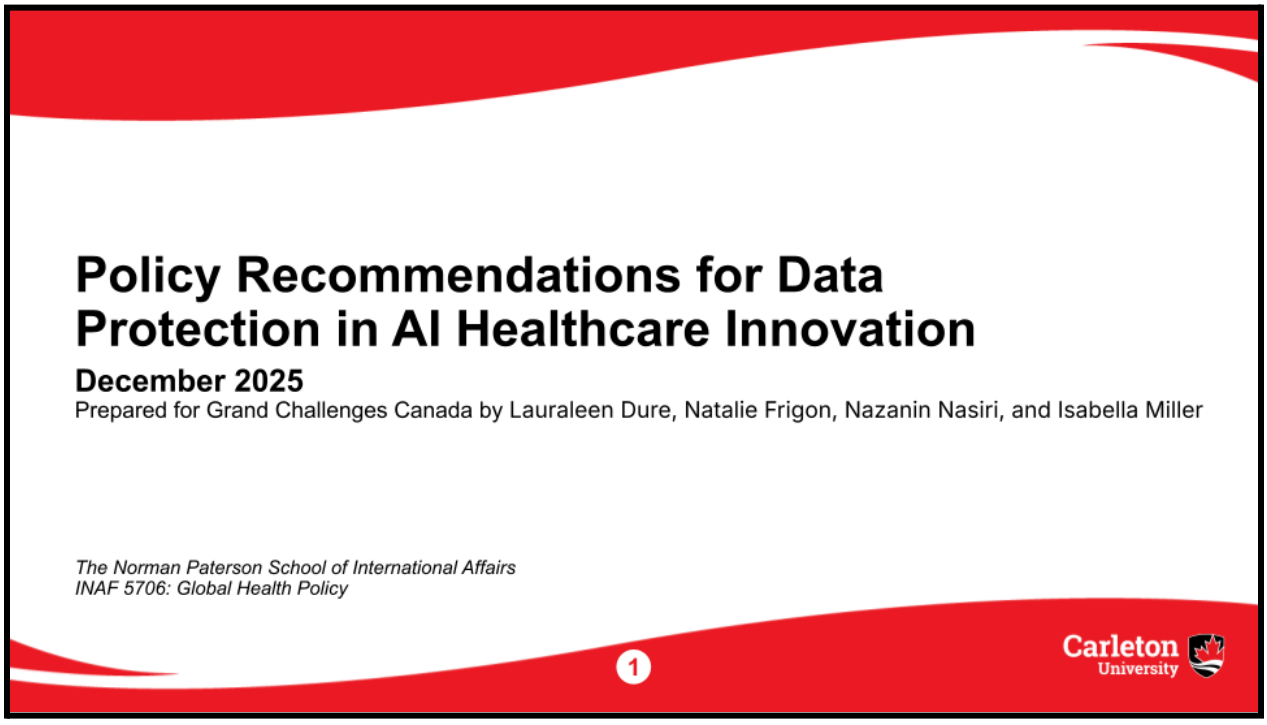
Data Protection Policy Recommendations for AI-Based Healthcare Systems in Low-Income Countries

Final Presentation Deck
Presented: December 15th, 2025
Submitted: December 15th, 2025

Prepared for: Grand Challenges Canada

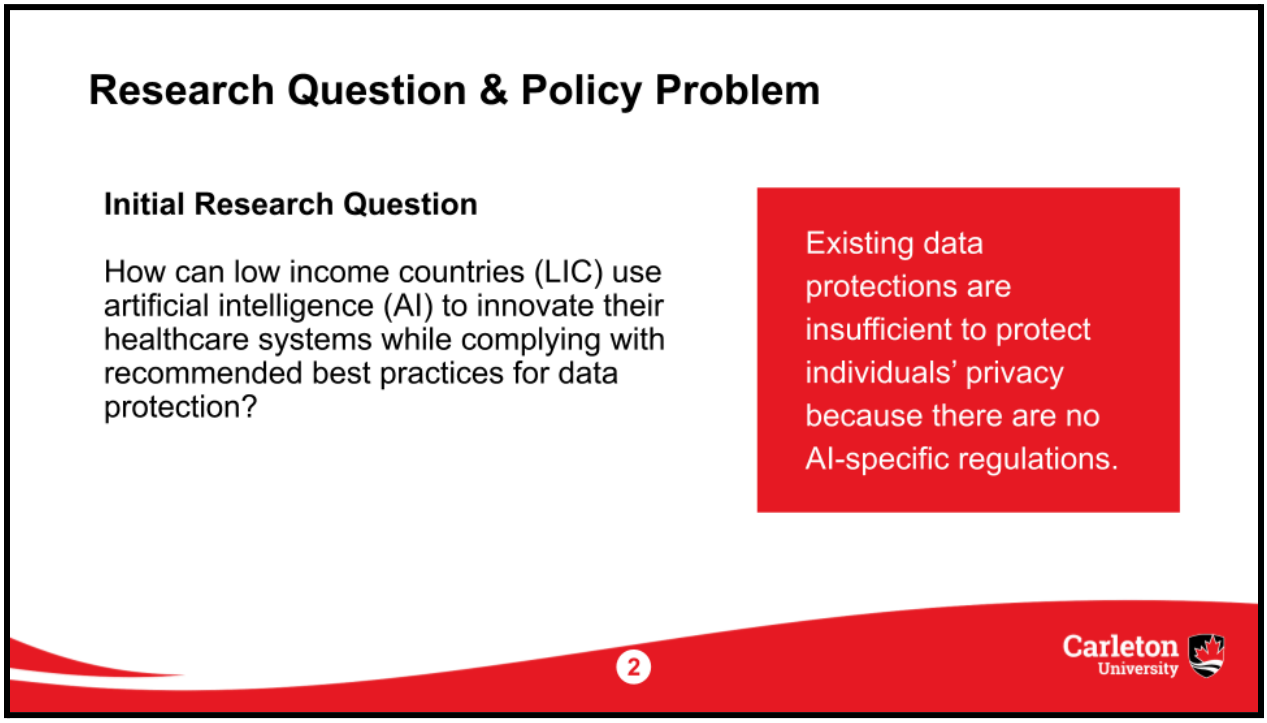
Lauraleen Dure, Natalie Frigon, Nazanin Nasiri, Isabella Miller

SLIDE ONE: Title Slide



Title: Policy Recommendations for Data Protection in AI Healthcare Innovation

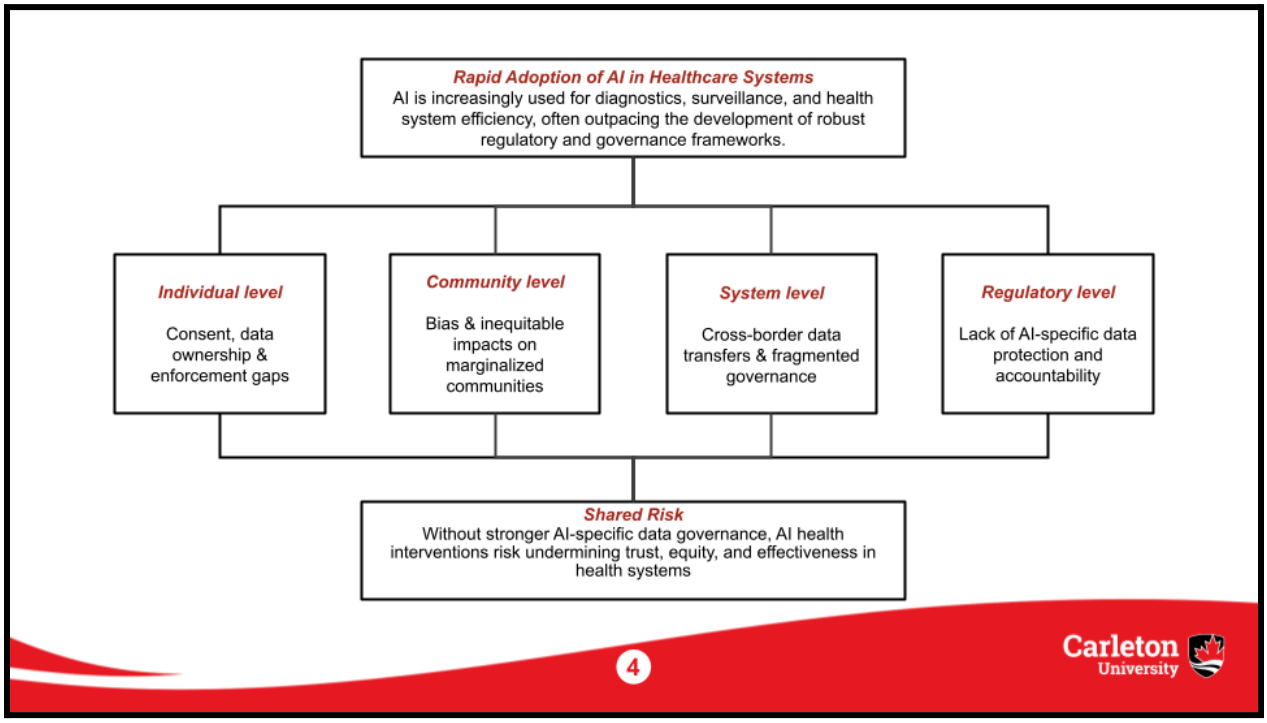
SLIDE TWO: Research Question & Policy Problem



Question: How can low income countries (LIC/LMIC) use artificial intelligence (AI) to innovate their healthcare systems while complying with recommended best practices for data protection?

Policy Problem: Existing data protections are insufficient to protect individuals' privacy because there are no AI-specific regulations.

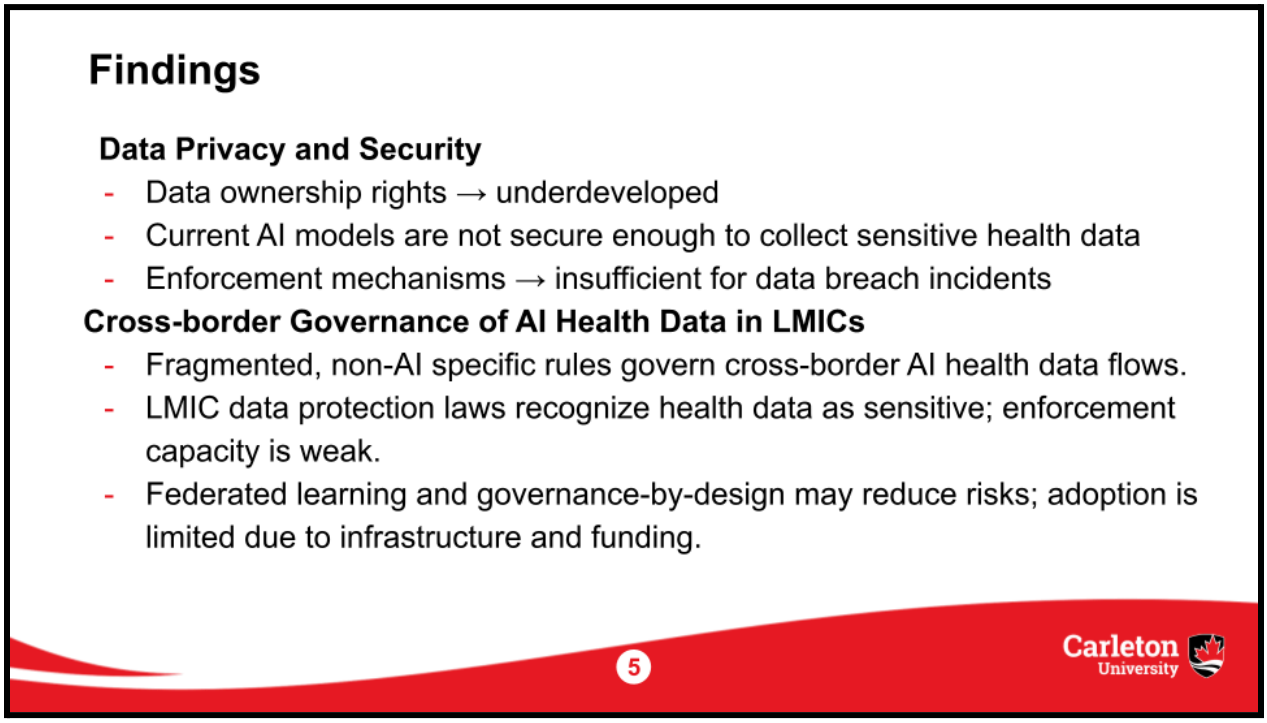
SLIDE THREE: Problem Framing



LMICs are increasingly integrating artificial intelligence (AI) to innovate healthcare delivery through diagnostics, disease surveillance, health prediction and patient engagement. However, this expansion is occurring within data protection systems that were not explicitly designed for AI-enabled, data-intensive or complex/non-transparent health interventions. Existing frameworks are fragmented, non-AI-specific and unevenly enforced, consequently creating gaps in consent, accountability, and oversight.

These gaps are particularly relevant in patients with stigmatized conditions or marginalized communities who already face structural barriers and increased risks from data misuse, bias, and exclusion. Additionally, many LMICs lack AI-specific regulatory frameworks and enforcement capacity, leading to limited safeguards when harms occur, including following data breaches. These issues are further reinforced through reliance on external vendors and cross-border health-data transfers, where fragmented governance weakens both individual privacy protections and national data sovereignty in practice.

SLIDE FOUR: Findings (1)



Data Privacy and Security

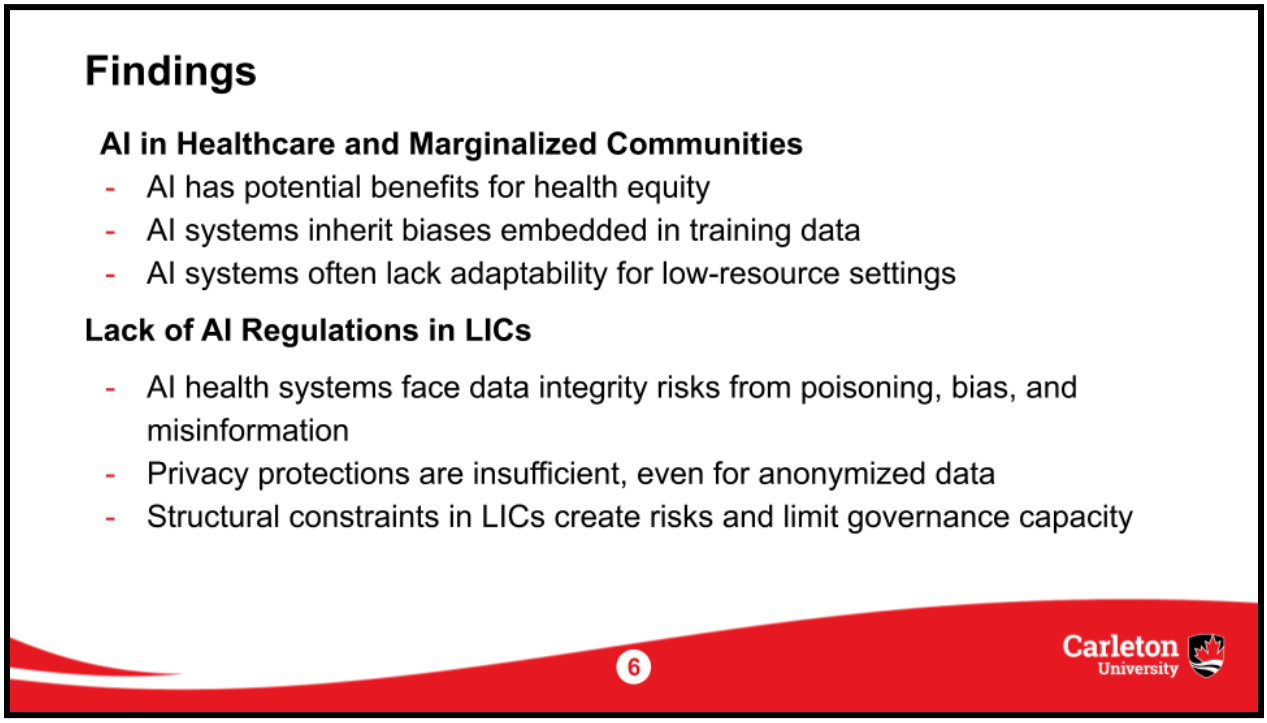
Data ownership rights are underdeveloped leaving patients unprotected. Informed consent is needed, but consent cannot be given if neither the patient or healthcare provider understands how the AI model collects and processes data. AI models are not secure enough to properly manage healthcare data. Healthcare data is inherently sensitive, and without more regulation on how AI models must store the data it collects, patients are vulnerable to a breach. If patients do not trust the technology, they are less likely to seek care. Enforcement mechanisms are ineffective and unprepared to deal with data breaches. Healthcare data is valuable, and vulnerable to cyberattacks. Private corporations are not often held accountable for data breaches because the lack of regulatory framework makes liability difficult to assign.

Cross-border Governance of AI Health Data in LMICs

Evidence shows that cross-border health-data transfers are central and involved in many AI-guided diagnostic and predictive tools used in LMICs, yet they are governed by a fragmented patchwork of global norms, regional frameworks, and national data-protection laws rather than AI-specific regulation. While many LMICs now classify health data as sensitive and formally recognize data-subject rights, limited regulatory capacity, weak enforcement, and legal uncertainty constrain effective protection in practice. As a result, governance of cross-border AI health data often defaults to private

contracts and external vendor infrastructures, shifting control away from public regulators, consequently weakening accountability and data sovereignty. Emerging approaches such as federated learning and governance-by-design architectures show promise in reducing cross-border risks, but adoption remains limited due to infrastructure, funding, and institutional capacity gaps.

SLIDE FIVE: Findings (2)



AI in Healthcare and Marginalized Communities

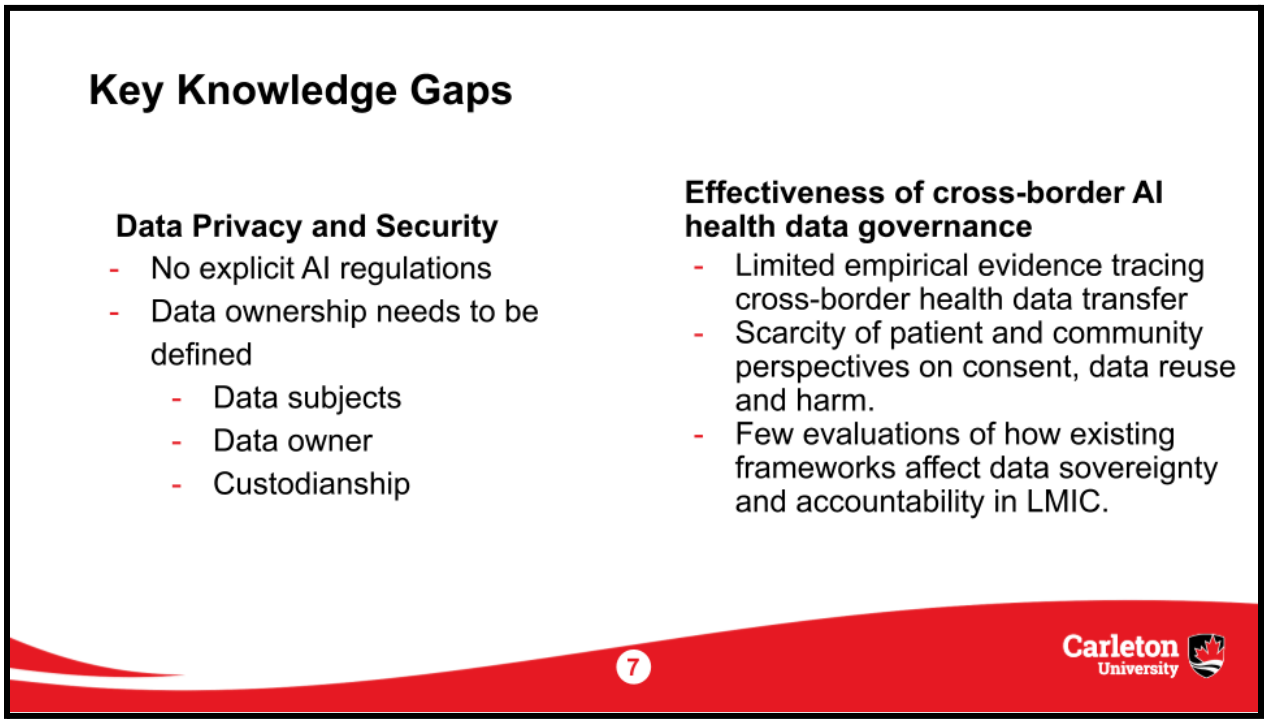
Firstly, in terms of health equity, AI has potential benefits for health equity, such as expanding access to care, automating tasks, and analyzing diverse health data to identify determinants of disparities and optimize resource allocation. However, AI also poses risks of perpetuating inequity, including algorithmic bias, lack of diverse data, and automation without ethical oversight, which can increase disparities and remove human judgment. Secondly, for biases, AI systems inherit biases embedded in training data, leading to discriminatory outcomes such as racial bias in risk prediction and poor performance in diagnosing conditions for darker skin tones. These biases amplify health disparities and require mitigation strategies like improving dataset diversity and ethical oversight. Lastly, AI systems improve efficiency in healthcare but often lack adaptability for low-resource settings and fail to incorporate diverse demographic data, leaving marginalized communities unacknowledged. Case studies (e.g., Rwanda and the Global South) reveal infrastructural limitations, lack of training, and uneven AI integration, highlighting the need for context-sensitive design and deployment.

Lack of AI Regulations in LICs:

AI Misuse and Data Integrity Risks: AI health interventions are vulnerable to data poisoning, biased datasets, and AI-generated misinformation, leading to hallucinations and inaccurate or inequitable health outcomes. *Privacy Threats and Security*

Vulnerabilities: Increased avenues for data collection increase exposure to privacy breaches including re-identification, reconstruction and property inference attacks. Anonymization alone does not protect sensitive health data. *Structural and Contextual Constraints*: There is weak technological infrastructure, severely underfunded cybersecurity sectors, regulatory gaps, and low digital literacy, which all impact the ability of LMIC health systems to protect data and govern AI health interventions.

SLIDE SIX: Key Knowledge Gaps (1)



Data Privacy and Security

We are so early in the implementation of AI systems in healthcare interventions, therefore most knowledge gaps are speculative based on hypothetical scenarios. There are currently no explicit AI regulations, so the efficacy of data protections are based on existing digital regulations. This knowledge gap demonstrates how inapplicable existing regulations are to sophisticated AI-models, making it not just a knowledge gap but a regulatory gap.

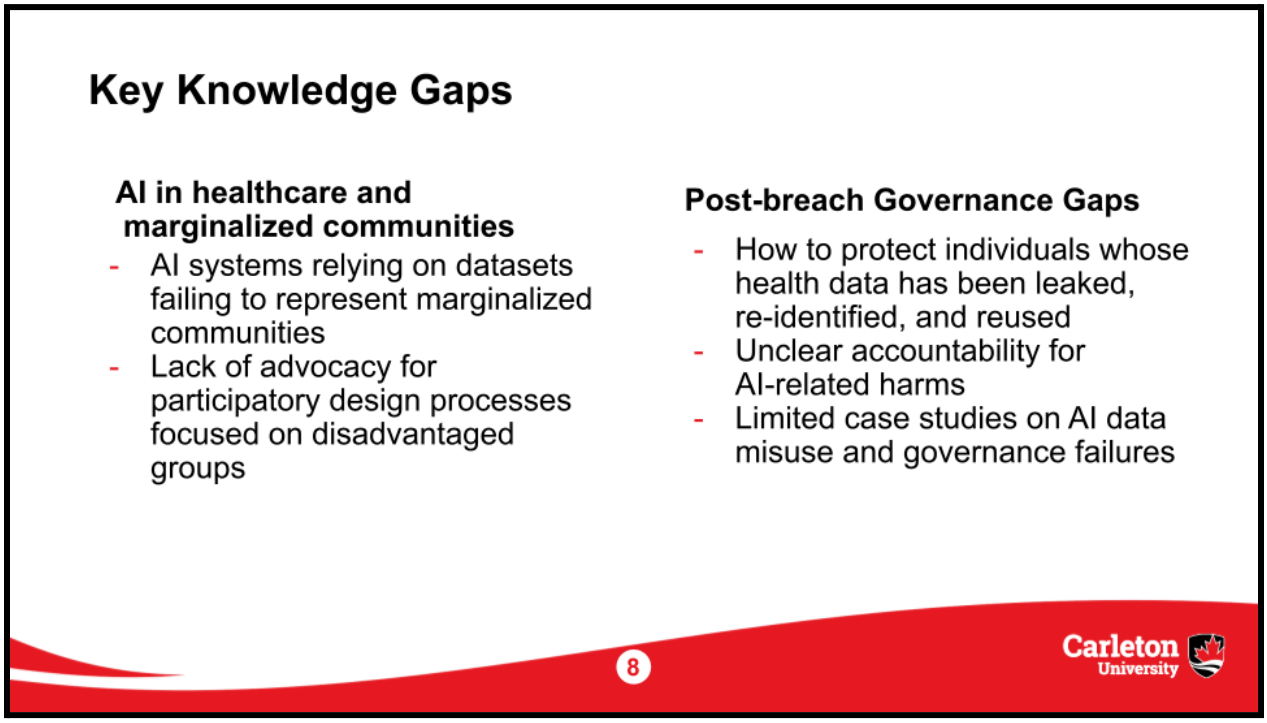
In existing and emerging regulations, there remains an issue of defining data ownership. In the medical context, data ownership does not always lie with the data subject. Custodianship must be directly addressed where the patient is a minor, unable to advocate for themselves, or when someone has power of attorney over them. Regulations must also consider if data protection carries on after a patient's death, especially when the information is biometric and could be attributed to family members.

Effectiveness of cross-border AI health data governance

Despite the growing body of global/regional/national guidance on cross-border health data governance, the evidence base still remains uneven. Most existing studies are conceptual, legal or policy-mapping analyses, with very limited empirical research tracing how health data actually move across borders in AI-enabled systems or how

these frameworks function in health practice. Additionally, patient and community perspectives particularly regarding informed consent, secondary data use and experiences of harm are not highly represented relative to regulator and institutional perspectives. Moreover, only a few studies evaluate whether current governance frameworks meaningfully strengthen data sovereignty, accountability or individual rights outcomes in LMIC settings. This lack of empirical evidence could limit policymakers' ability in assessing which governance approaches work in health practice and where reforms are most urgently required.

SLIDE SEVEN: Key Knowledge Gaps (2)



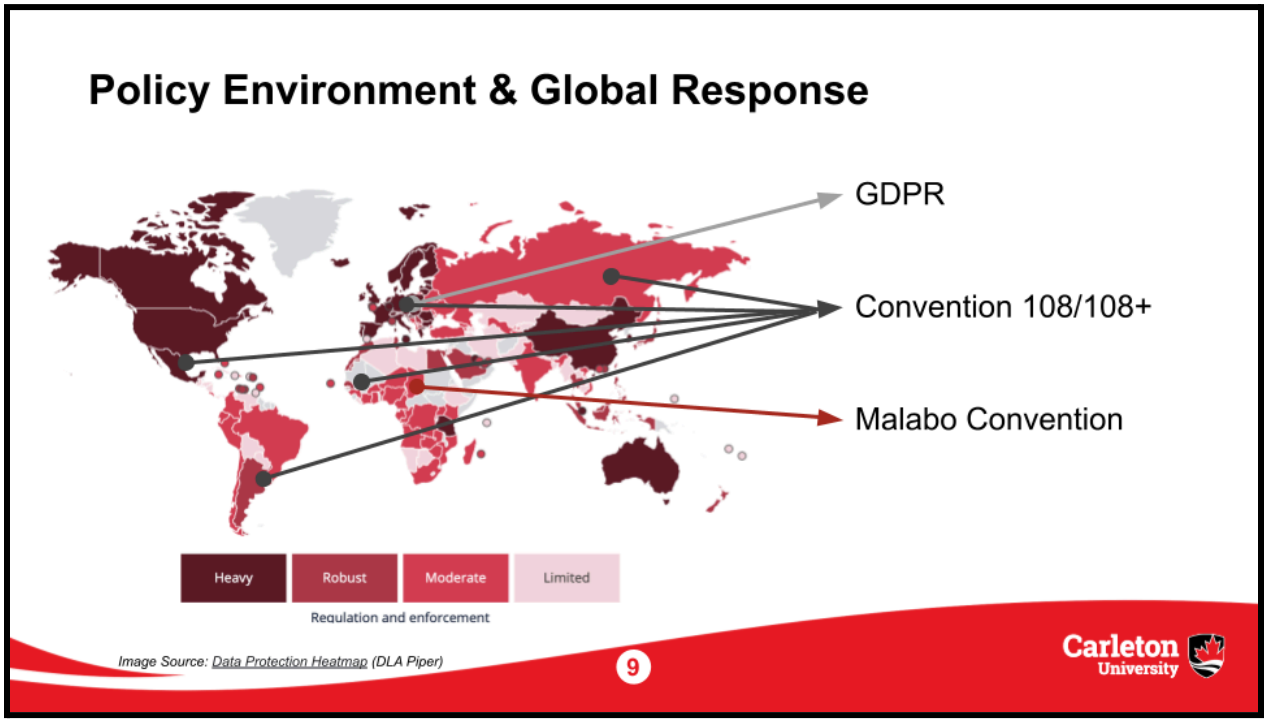
AI in healthcare and marginalized communities

There are two main knowledge gaps. 1) Lack of diverse and inclusive data: AI systems often rely on datasets that fail to represent marginalized communities adequately. This underrepresentation leads to blind spots in model performance, especially for racial and ethnic minorities, and can perpetuate systemic inequities. 2) Participatory Design: There is a lack of advocacy for participatory design processes that center the voices of disadvantaged groups in AI governance, ensuring technology aligns with community values and priorities.

Post-breach Governance Gaps

Most research focuses on preventing data breaches and there is very little research on what happens after sensitive health data has been leaked, re-identified, or reused in AI systems. Additionally, there is a lack of clarity surrounding accountability. Who is responsible when AI health systems cause harm due to privacy, bias, and misinformation, especially in LMIC contexts with weak enforcement capacity. Lastly, there is limited research on real-world cases where people have been harmed by weak data protection in AI health interventions; very little evidence of how governance failures occur and impact communities.

SLIDE EIGHT: Policy Environment & Global Response



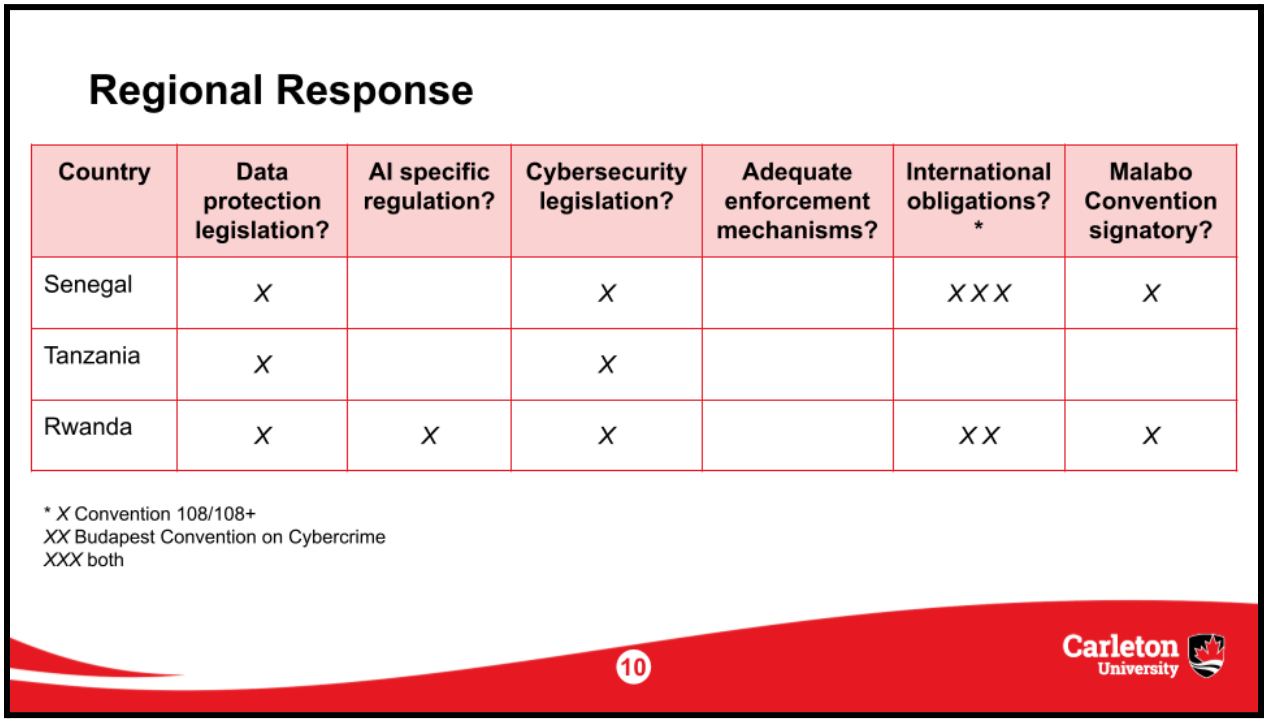
European Union General Data Protection Regulation is the gold standard of data protection, and can be applied extraterritorially. It has specific definitions, especially for health data. The Data Protection Authorities (DPAs) have full authority to investigate and issue hefty fines for non-compliance. GDPR has strong breach notification rules specifically for healthcare breaches, and has the principle of data minimization to ensure that only data that needs to be collected is collected. The GDPR also establishes the 'right to explanation' which should include the rationale behind decisions made by AI models.

Convention 108+ is the Convention on the protection of individuals with respect to the processing of personal data, the first binding international instrument that protects individual rights during data collection and processing, and regulates cross-border flow of personal data. It has adequacy requirements and auditing measures to ensure compliance of member states.

The African Union Convention on Cybersecurity and Personal Data Protection, known as the Malabo Convention, puts an emphasis on consent as a legal basis for data processing, using principles from the GDPR. Africa is the first regional union outside of Europe to adopt a data protection Convention. Member states must establish

independent national data protection authorities to monitor and enforce legislative compliance, receive concerns from data subjects, and sanction violations.

SLIDE NINE: Regional Response

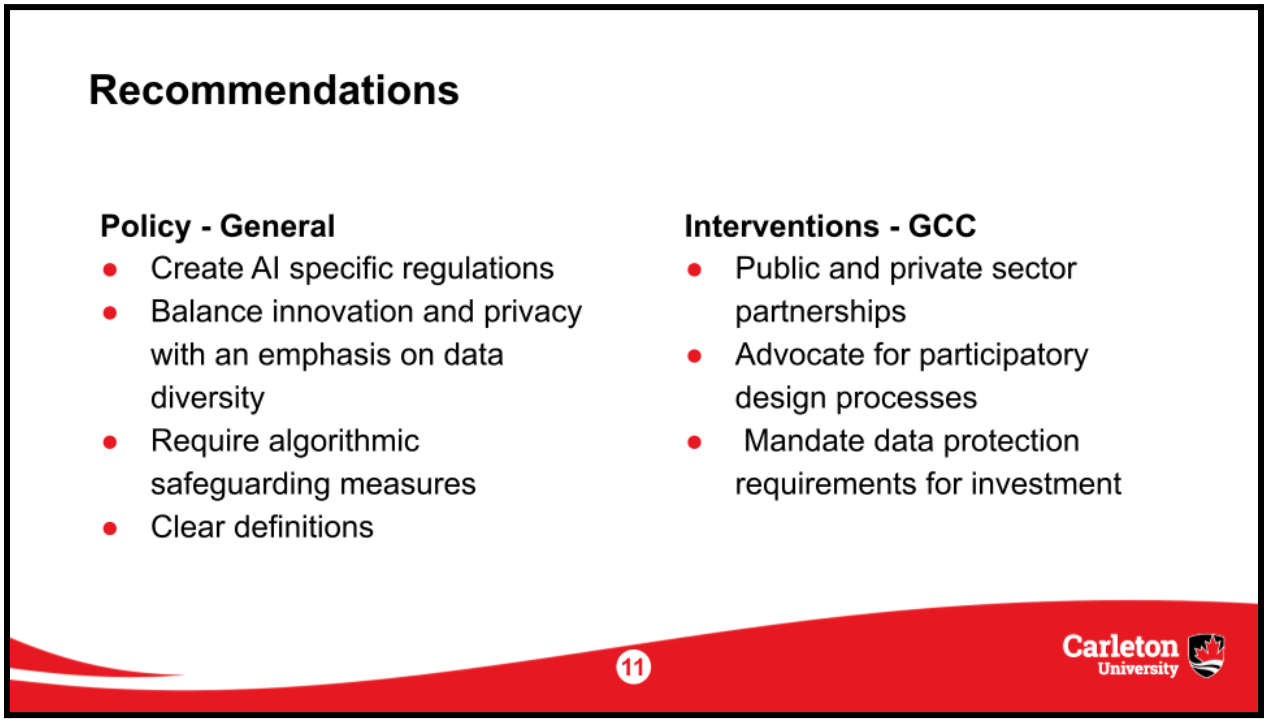


Senegal is a leader in adopting international instruments for data protection, but it does not have a specific AI policy yet, although one is proposed through their "Digital Senegal 2025" initiative. Their data protection law prohibits the collection of health data unless the data subject has given their consent, and the Penal Code prohibits non-consensual collection of health data and data subjects should be made aware of their rights.

Tanzania established the Personal Data Protection Act (PDPA) (2022) and the Personal Data Protection Commission (PDPC), and broadly defines personal and sensitive data. The framework remains vague and has weak enforcement mechanisms, especially since the compliance enforcement agency (PDPC) is closely linked to the government and has limited capacity. There is no formalized system for compliance monitoring or clear requirements for enforcement. Gaps are compounded by severe underfunding in cybersecurity and the digital divide.

Rwanda is one of the first African nations to implement an AI policy. Rwanda has a Data Protection Law, Cybercrime Law, and ICT Law.

SLIDE TEN: Recommendations



General Policy Recommendations

Countries should:

- Create AI specific regulations that can address the unique challenges this technology presents in healthcare contexts
- Balance innovation and privacy, so models can still be trained on diverse data sets
- Require algorithmic safeguarding measures for AI models
- Regulation should include clear definitions for data subject, data custodianship, and data ownership

Interventions recommended for GCC

60% of healthcare funding in Africa comes from private actors, and AI systems for healthcare are increasingly becoming commercialized. Without rigorous oversight, it could bring harm to communities through healthcare interventions and degrade the levels of healthcare that are provided in the Global South. Public-private partnerships are necessary to have proper enforcement because 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.

GCC can strengthen the safety and effectiveness of AI health interventions by setting minimum data protection standards as a condition of funding, such as decentralized data storage and data minimization. Funded projects would be responsible for implementing privacy-preserving AI designs, post-breach notification, harm-mitigation plans, and clear guidance for data subjects (patients) and healthcare providers on data rights and best practices. By setting these expectations at the funding stage, GCC can help shape responsible AI use in LICs.

SLIDE ELEVEN: Conclusion