A guiding framework for creating a comprehensive strategy for mHealth data sharing, privacy, and governance in low- and middle-income countries (LMICs)

Rada Hussein, Ashley C. Griffin, Adrienne Pichon, and Jan Oldenburg

1Ludwig Boltzmann Institute for Digital Health and Prevention, Salzburg, Austria, 2Department of Health Policy, VA Palo Alto Health Care System, Stanford University School of Medicine, Stanford, California, USA, 3Department of Biomedical Informatics, Columbia University, New York, New York, USA, and 4Participatory Health Consulting, LLC, Richmond, Virginia, USA

Corresponding Author: Rada Hussein, PhD, FIAHSI, Ludwig Boltzmann Institute for Digital Health and Prevention, Lindhofstraße 22, 5020 Salzburg, Austria; rada.hussein@dhp.lbg.ac.at

ABSTRACT

With the numerous advances and broad applications of mobile health (mHealth), establishing concrete data sharing, privacy, and governance strategies at national (or regional) levels is essential to protect individual privacy and data usage. This article applies the recent Health Data Governance Principles to provide a guiding framework for low- and middle-income countries (LMICs) to create a comprehensive mHealth data governance strategy. We provide three objectives: (1) establish data rights and ownership to promote equitable benefits from health data, (2) protect people through building trust and addressing patients’ concerns, and (3) promote health value by enhancing health systems and services. We also recommend actions for realizing each objective to guide LMICs based on their unique mHealth data ecosystems. These objectives require adopting a regulatory framework for data rights and protection, building trust for data sharing, and enhancing interoperability to use new datasets in advancing healthcare services and innovation.

Key words: data governance, digital health, global health informatics, mHealth, sustainable development goals (SDGs)

INTRODUCTION

The Coronavirus pandemic (COVID-19) has rapidly accelerated the global adoption of mobile health (mHealth) devices and software, which have become central public health tools for health monitoring, telemedicine, and surveillance. According to the World Health Organization (WHO), mHealth is defined as “the use of mobile wireless technologies for public health,” which encompasses a vast array of tools to support health such as mobile phones, wearable sensors, and video applications (apps). mHealth tools have been increasingly used in low- and middle-income countries (LMICs), particularly short messaging service approaches, with evidence suggesting effective delivery of health information to patients for disease management and support for healthcare workers. The United Nations has also incorporated mHealth into their Sustainable Development Goals to address global challenges such as poverty and the lack of universal health coverage. While use of mHealth data has demonstrated positive impacts in public health planning and response, data governance regulations have lagged behind innovation. For example, with the wide use of contact-tracing apps, data sharing is a complex issue regarding which types of data are collected, how they are stored, for how long, and who has access. Some governments have endorsed apps that track individuals during quarantine or even enforce quarantine by asking individuals to submit “selfies.” These challenges span a number of domains, including data privacy, ownership, protection, consent, and ethics. LMICs are notably faced with these challenges as many lack digital data governance strategies.

© The Author(s) 2022. Published by Oxford University Press on behalf of the American Medical Informatics Association. All rights reserved. For permissions, please email: journals.permissions@oup.com
Careful consideration of data governance and regulatory issues in LMICs is essential to realize the full promise of mHealth to improve health outcomes and delivery.\textsuperscript{18,19}

To address some of these challenges, several frameworks and strategies have been developed to guide health data regulation and governance.\textsuperscript{15,20} For example, the WHO global strategy on digital health (2020–2025)\textsuperscript{21} set a strategic objective for digital health governance at national and international levels through the creation of sustainable and robust governance structures, including regulatory frameworks. The Lancet Commission also developed a conceptual framework on digital technologies as new determinants of health.\textsuperscript{10}

The framework includes data governance as one of ten potential enablers of digital health future readiness, with emphasis on equity and human rights. Additionally, key elements of digital data governance have been outlined to protect and promote well-being of vulnerable populations in LMICs.\textsuperscript{20} In this article, we build upon this body of existing work to create an mHealth data governance framework with a set of recommended actions for LMICs.

**HEALTH DATA GOVERNANCE PRINCIPLES**

In April 2022, the Health Data Governance Principles\textsuperscript{22} were created to universalize the benefits of digital health through protecting people, promoting health value, and prioritizing equity. These principles, developed in partnership with more than 200 digital health experts from over 130 global organizations, are the first global set of principles developed to guide the use of data in health systems (Figure 1). The principles are grounded in human rights and equity to support public health systems that can deliver healthcare broadly. They balance the rights of individuals with the rights of organizations and public health. This creates a common vision where people and communities can share, use, and benefit from health data. Drawing upon these principles, we provide tailored objectives and recommendations, encompassing tools and guiding examples, that could be used to guide LMICs in mHealth data governance (Table 1). This work was conducted by members of the Health Level Seven International (HL7\textsuperscript{75}) Patient Contributed Data group, which focuses on identifying principles and rights for patients and their data as well as assessing standards that impact patient contributed data.

Objective 1: prioritize equity through establishing mHealth data rights and ownership

mHealth data governance should be based on strong and clear data-related rights, including the basic human rights to protection, safety, and to benefit equitably from data contributed at individual and community levels. Indigenous researchers in the United States have put forth recommendations for considering ethics around health research and data that center on group-level concerns and tribal autonomies and sovereignties, aligning with Indigenous communitarian ethics, rather than “Western” individualistic ethics.\textsuperscript{23}

Define mHealth data governance roles and responsibilities

To ensure mHealth data rights and ownership, it is valuable to define various mHealth data roles within health data systems in light of a data protection framework, including: data owner, data custodian, data processor, data steward, data trustee, and data use beneficiary. Establishing roles helps to clarify who has the right to do what and who must ensure these rights are upheld.

At a national or regional level, a regulatory framework using existing data governance guidelines, such as in the European Union’s (EU) General Data Protection Regulation (GDPR),\textsuperscript{24} should identify:

1. rights and roles of primary mHealth data actors (individuals, family members, caregivers, healthcare providers).
2. ownership of different types of mHealth data (patient-generated health data, health records, app or device-produced data, etc.).

Codify mHealth data rights and ownership

The identified rights and ownership should be codified in legislation and policy in alignment with current national (regional or global) data protection regulation frameworks. These should include definitions of ownership, for example: mHealth data are owned by the individual, community providing the data, healthcare providers. They also should incorporate related rights such as the right to control the use of data, decline participation in data collection, withdraw data from a system, and to obtain benefit.

mHealth data ownership implies that individuals have a right to know, determine, and control how their data are used, and to benefit equitably from such data. The right to access data is different from owning that data, which may vary according to mHealth data types and the linked stakeholders’ roles and responsibilities.

Extend data rights and ownership to products and services

The identified mHealth data rights and ownership model should be extended to related products and services. For example, the secondary use of research also should not cause harm to individuals or communities.\textsuperscript{25,26} Similarly, individual and community ownership over their data extend to the right to equitable benefit-sharing from the products and services built from their contributed data. Services built from the data might include artificial intelligence (AI) products or reselling personal data for profit by a third party.

Guiding example

The EU GDPR stimulated a global discussion about data privacy and protection and specified how organizations must deal with personal identified data. Currently, many jurisdictions are moving towards GDPR-compatible regimes. The GDPR identifies principles relating to the processing of personal data: (1) lawfulness, fairness, and transparency, (2) purpose limitation, (3) data minimization, (4) accuracy, (5) storage limitations, (6) integrity and confidentiality, (7) accountability, (8) international transfer. The GDPR rights of the data subject are: (1) right to be informed, (2) right of access, (3) right to rectification, (4) right to object to processing, (5) right to object automated decision-making, (6) right to be forgotten, (7) right to data portability, (8) right to restrict processing.

Tiffin et al\textsuperscript{20} provided a practical checklist for implementing digital data governance principles derived from their experiences working with digital health data in LMICs. They examined four key domains: ethics and informed consent, data access, sustainability, and legal framework.

Objective 2: protect people through building trust (patients’ perspective on mHealth data)

Building trust in data systems and practices requires the codevelopment of mHealth governance systems in a participatory and transparent manner with individuals and communities.\textsuperscript{27,28} The covering regulations and guidelines should be accessible, understood, and followed in practice to build trust. Trust requires safeguarding data,
ensuring privacy, and establishing transparent and inclusive data collection, processing, storage, analysis, use, sharing, and disposal processes.

Key patient concerns relate to data privacy and security and how researchers and companies will use their data, which may prevent patients from sharing their data. Willingness to share data is impacted by the degree of trust in the entity and its policies, as well as concerns about downstream use of the data. In LMICs, data mishandling or reidentification could stigmatize communities or populations.

Establish transparent and accessible processes and systems
Transparency in mHealth data governance is required to create buy-in from stakeholders, particularly patients, around data processes. The Data Futures Partnership in New Zealand defines transparent data use with three dimensions: value, protection, and choice. Accordingly, stakeholders can understand how and why data are collected (value); how data are stored, analyzed, and used (protection); and how the systems and processes that support data governance operate (choice).

Guiding example
The Digital Health Europe project introduced a framework for citizen-controlled data sharing to motivate citizens to share their own data. On the policy level, the framework addresses transparency, information, awareness, and trust-building. Technically, it focuses on datasets, tools, and interoperability. LMICs could leverage a similar individual-controlled data sharing model to facilitate trust and mutual reciprocity.

Objective 3: promote health value through enhancing systems and services (health system’s perspective on mHealth data)

mHealth data governance can enable meaningful use of data to enhance health system efficiency and resilience. Data can actively contribute to the transformation of health systems into value-based systems. Embedding these principles in LMIC environments can facilitate the development of equitable and efficient health systems.

Evaluate the benefits of mHealth data
The secondary use of mHealth data in medical research and policy-making has demonstrated the potential to advance medical sciences, public health services, and healthcare innovation, especially when AI tools are used to analyze the information. Consequently, stakeholders legitimately require appropriate, secure access to data. Citizens who contribute data must also understand how their data may contribute to research and development.
<table>
<thead>
<tr>
<th>Health data governance principles</th>
<th>Objectives</th>
<th>Recommended actions for mHealth data governance in LMICs</th>
</tr>
</thead>
</table>
| Prioritize equity | Objective 1: Prioritize equity through establishing mHealth data rights and ownership | • Prioritize accessible, low technology solutions (such as text messaging) that can be widely dispersed  
• Promote policies that ensure equal access to mHealth tools and capabilities (broadband access, smartphone access, etc.)  
• Enable patients and communities to govern how their data are shared and with whom  
• Consider ethics aligning with Indigenous communication (beyond just the legal frameworks) in terms of respect for sovereignty, solidarity, beneficence, and justice as part of building trust and partnerships. This could be realized through, eg, inclusivity of Indigenous perspectives, establishment of tribal research regulatory structures, informed consent structures that consider both community and individual viewpoints and mandate reconsent for new research questions etc. |

**Used framework:** EU GDPR  
**Guiding example:** A checklist for implementing digital data governance principles

| Protect people | Objective 2: Protect people through building trust and representing the patients’ perspective on mHealth data | • Require third-party apps and devices to request a person’s permission before sharing or reselling their data  
• Require transparent, clear disclosure of the way the data will be stored and used  
• Enable users to modify and retract data sharing permissions  
• Educate individuals about using mHealth, potential risks of unprotected data, and data protection strategies |

**Used tool:** The Data Futures Partnership in New Zealand  
**Guiding example:** Digital Health Europe project

| Promote health value | Objective 3: Promote health value through enhancing systems and services representing the health system’s perspective on mHealth data | • Enable individuals to share personal data with health systems  
• Label provenance of data elements, including data shared by patients  
• Simplify sharing data for purposes of collaboration around individual and community health  
• Develop principles governing secondary use of health data to protect individuals and promote medical discovery |

**Used tool:** The WHO guidance on the ethics and governance of AI in health  
**Guiding example:** principles and norms governing responsible data sharing in international health research

**Next steps**  
Step 1. Use this framework and the provided guiding examples to create a national/regional mHealth governance strategy in LMICs.  
Step 2. Follow the user guide of the Health Data Governance Principles (https://healthdataprinicples.org/use) to identify how different stakeholders can properly implement this framework. The different stakeholder groups addressed in this user guide include governments, communities, youth organizations, research institutes, private sectors, donors, international organizations, and others.

**Examples on how to use this framework in LMICs**  
**Step 2 selected examples:**  
**All stakeholder groups** in LMICs have to first publicly endorse the equity and human rights-based Health Data Governance Principles to guide the collection and use of mHealth data, at national, regional, and international levels.  
**Governments** in LMICs can adopt the described framework to update (or develop) national and subnational legislation, regulation, policy frameworks, and practices on mHealth data governance. This will be followed by a call on WHO to lead the development of global health data governance.  
**Technology companies and the private sector in LMICs** can update organizational policies and practices for mHealth data by incorporating the created mHealth governance strategy (in Step 1).
Guiding example
Kalkman et al. conducted a systematic review of the principles and norms governing responsible data sharing in international health research. They identified four themes (societal benefits and value; distribution of risks, benefits, and burdens; respect for individuals and groups; and public trust and engagement) under which relevant principles and norms are grouped (Table 2). This work could lead to the development of a harmonized governance framework for data sharing in health research.

Promote data sharing and interoperability
Interoperability initiatives have demonstrated secure mHealth data sharing between systems. Concepts like data portability, open data, community data, data trustees, and data exchanges could also be considered part of the data sharing and interoperability mechanism.

Knudsen highlighted the following five principles to achieve better data interoperability:

1. Principle 1: Healthcare providers need access to data beyond silos.
5. Principle 5: Data must be shared using industry standards, such as HL7 Fast Health Interoperability Resources (FHIR).

Recently, the FHIR for FAIR (Findable, Accessible, Interoperable, and Reusable) implementation guide was introduced to provide guidance on how HL7 FHIR can be used for supporting FAIR health data implementation and assessment. However, data interoperability currently applies primarily to data collected originally by health systems and needs to be extended to mHealth data collected through apps and devices.

Facilitate innovation using mHealth data
mHealth tools can provide novel and real-time data into clinical care, although large-scale successes remain elusive. With these datasets, AI and big data analytics can be applied, leading to new tools, innovative healthcare services, and health insights at individual and population levels. This requires developing a governance environment that can enable innovation and effectively support the application of new digital technologies, as well as new kinds of data uses.

Guiding report
The WHO recently published guidance on the ethics and governance of AI in health. The report identified six core principles to mitigate ethical challenges and risks: (1) protect autonomy; (2) promote human well-being, human safety, and the public interest; (3) ensure transparency, explainability, and intelligibility; (4) foster responsibility and accountability; (5) ensure inclusiveness and equity; (6) promote AI that is responsive and sustainable.

CONCLUSION
mHealth has demonstrated strong potential to advance medicine, healthcare services, and innovation globally. As the volume of mHealth devices continues to grow and new data streams emerge, global stakeholder engagement is needed to implement and maintain mHealth data governance in LMICs. The Health Data Governance Principles provide a base for harmonizing and creating data governance strategies internationally. Leveraging this framework, we identified relevant objectives for mHealth data protection, sharing, and interoperability. To realize these objectives, collaborative participation from patients, communities, health systems, and governments is essential for improving global health equity and outcomes.
This perspective received no specific grant from any public, commercial, or not-for-profit funding agency. ACG is currently supported by a VA Advanced Fellowship in Medical Informatics. The opinions expressed are those of the authors and not necessarily those of the Department of Veterans Affairs or those of the United States Government. AP is supported by Funding Award No. T15 LM007079.

AUTHOR CONTRIBUTIONS
RH wrote the first draft of the manuscript. ACG, AP, and JO made substantial edits and contributions and approved the final version of the manuscript.

ACKNOWLEDGMENTS
The authors thank other members of the Patient Contributed Data group (sponsored by the HL7 Patient Empowerment workgroup) for their valuable comments and fruitful discussions.

CONFLICT OF INTEREST STATEMENT
None declared.

DATA AVAILABILITY
No new data were generated or analyzed in the context of this article.

Figure 3. Framework for citizen-controlled data sharing (Source: Digital Health Europe project).33

Table 2. Themes and principles for responsible health data sharing (adapted—Source: Kalkman et al41)

<table>
<thead>
<tr>
<th>Main themes</th>
<th>Norms and principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Societal benefits and value</td>
<td>Accessibility, Data quality, Sustainability, Scientific progress/value, Promote health and well-being, Interoperability, Scientific validity, Societal benefit, Duty to share, Collaboration and capacity building, Health-related public interest, Improved clinical care, Enhance healthcare decision-making, Social value, Individual benefit, Improve public health, Efficiency.</td>
</tr>
<tr>
<td>Distribution of risks, benefits and burdens</td>
<td>Benefit-sharing, Reciprocity, Risk-benefit evaluation, Equity and fairness, Protection of intellectual property, Attribution, Proportionality, Ownership, Recognition and attribution.</td>
</tr>
<tr>
<td>Respect for individuals and groups</td>
<td>Respect/protect privacy, Protect confidentiality, Ensure data security, Respect individuals, Respect individual rights, Individual autonomy, Respect dignity of individuals, Respect (the dignity of) communities, Prevent discrimination, Legal compliance, Protect life, health and well-being, Respect families, Respect welfare of individuals.</td>
</tr>
<tr>
<td>Public trust and engagement</td>
<td>Transparency, Accountability, Engagement/participation, Maintain public trust, Maintain integrity, Responsibility, Professionalism, Health democracy, Solidarity.</td>
</tr>
</tbody>
</table>
REFERENCES