



Challenges and Recommendations
in Data Governance
**FOR THE DEVELOPMENT OF
ARTIFICIAL INTELLIGENCE
IN HEALTH IN LATIN AMERICA
AND THE CARIBBEAN**

CONTENT

TEAM	3
EXECUTIVE SUMMARY	4
GLOSARRY	7
01. INTRODUCTION	8
02. HEALTH DATA GOVERNANCE: WHY DOES IT MATTER?	9
GLOBAL AND REGIONAL INITIATIVES	12
WHAT ARE THE HEALTH DATA GOVERNANCE PRINCIPLES?	17
03. HEALTH DATA GOVERNANCE AND AI IN LATIN AMERICA AND THE CARIBBEAN	24
WHAT IS THE SCENARIO IN THE REGION?	24
WHAT ARE THE MAIN CHALLENGES?	29
WHAT DO WE RECOMMEND?	31
04. CONCLUSIONS	33
05. ACKNOWLEDGEMENTS	34
06. BIBLIOGRAPHY	35
07. ANNEX	38

TEAM

SOFÍA PIRSCH: Bachelor in Political Science (UBA). Graduate in Advanced Studies of Gender, Culture, and Power (Universidad de San Martín). Candidate for a Master's in Political Science (Universidad Torcuato Di Tella) and in Clinical Effectiveness (UBA). Research Fellow at CIIPS-IECS.

MARTÍN SABÁN: Pediatrician (UBA). Member of the Information and Communication Technologies subcommittee of the Argentine Society of Pediatrics. Candidate for a Master's in Clinical Effectiveness (UBA). Research Fellow at CIIPS-IECS.

DANIEL RIZZATO LEDE: Medical Doctor (National University of Cuyo). Specialist in Internal Medicine (HB-UBA) and Health Informatics (IUHIBA), with experience in Digital Health implementations and public health management. Digital Health Consultant at CIIPS-IECS.

CINTIA CEJAS: Bachelor in Political Science (UCA) and Master in Social Sciences and Health (FLACSO-CEDES). Specialist in health project management. Coordinator of the Center for Implementation and Innovation in Health Policies (CIIPS-IECS) and the Center for Artificial Intelligence in Health for Latin America and the Caribbean (CLIAS).

EXECUTIVE SUMMARY

The document "Challenges and Recommendations in Data Governance for the Development of Artificial Intelligence in Health in Latin America and the Caribbean" aims to analyze the current state of data governance and the progress of AI in the health sector in the region, identify key challenges, and propose tools to overcome them. **The analysis is framed within the Health Data Governance Principles.**

HOW CAN PROPER DATA GOVERNANCE CONTRIBUTE TO THE DEVELOPMENT OF RESPONSIBLE, EQUITABLE, REPRESENTATIVE, AND PEOPLE-CENTRIC AI IN HEALTH, PRIORITIZING THE PROTECTION OF THEIR RIGHTS?

- Ensuring data quality to provide high-quality inputs for algorithm development.
- Facilitating broad and ethical access to datasets, enabling developers and researchers to advance innovative AI solutions.
- Guaranteeing data privacy and confidentiality, building the necessary trust for individuals to share their data.
- Promoting transparency in the use of health data, crucial for gaining public acceptance and trust.
- Fostering data interoperability among health systems to broaden the range of information available for AI model creation.
- Providing incentives and structures for collaboration among institutions, researchers, and companies, encouraging joint innovation in AI in health.
- Facilitating data standardization, allowing AI models to be consistently applied in different contexts and locations.
- Addressing bias management in data, promoting equity, justice, and representativeness in the results of AI models applied to health.
- Safeguarding individual and collective rights in the use of health data to train AI models, ensuring the protection of privacy and autonomy.

In this regard, the **challenges in Latin America and the Caribbean (LAC)** can be summarized as follows:

- **Regulatory:** The countries in the region lack adequate regulatory frameworks for the protection of individuals' and communities' data.
- **Data Quality:** Available repositories in the region are scarce, and data often exhibit low quality and various biases, posing risks of deepening existing inequalities.
- **Infrastructure:** LAC countries face deficiencies in infrastructure for the development of responsible AI solutions, such as inequitable access to the internet or insecure information systems.

- **State Capacities:** The absence of specialized agencies for data use, coupled with states' inability to efficiently guarantee the protection and security of individuals' data, is a challenge for many countries in the region.
- **Collaboration among Stakeholders:** LAC countries have the opportunity to move towards common strategies not only among states but also with companies, universities, and other stakeholders to define common parameters for the use and exchange of data.

Based on these challenges, the following recommendations are presented for countries in the region:

REGULATORY

- Develop comprehensive, clear, up-to-date, flexible and reliable regulatory frameworks on data governance that ensure both data protection and the promotion of innovation. These frameworks should include specific considerations for addressing and safely using health data.
- Regulations should anticipate data protection in the context of data aggregation for the construction of population profiles.
- Incorporate data governance in health at different levels of the healthcare system, not only at the government level but also within hospitals, care centers, universities, and any relevant institutions.

DATA QUALITY

- Promote the collection and use of local data aligned with the context of countries in the region, including demographic and epidemiological profiles. This approach ensures the generation of higher-quality solutions that are more representative of local populations seek to reduce and control biases throughout the development of AI projects.
- Encourage the generation of updated public databases with complete and high-quality data.
- Provide training for individuals working with data at any stage of the data cycle to ensure data quality is preserved.
- Incorporate elements of data use and management into the educational curricula of healthcare professionals in training.

ETHICAL

- Address ethical issues from the early stages of project design through implementation and monitoring.
- Involve ethics experts and professionals from various disciplines from the beginning of projects to mitigate biases.
- Strive for the anonymization of health data, secure hosting and temporary, compartmentalized archiving.
- Collect data to answer a specific research question.

INFRASTRUCTURE

- Encourage both domestic and foreign investment in digital infrastructure.
- Design comprehensive cybersecurity plans that include experts from different disciplines to achieve a holistic perspective, including the healthcare sector.

STATE CAPACITIES

- Promote the establishment of specialized agencies focused on data use and protection, privacy, and access to information, ensuring these agencies have experts in health data.
- Encourage the formation of a specialized state bureaucracy in data use and health data utilization.
- Develop manuals, guidelines, or best practices guides so that developers of AI applications in health are aware of the governmental processes they must follow to develop an AI solution in health.
- Promote the design and implementation of National Digital Health Strategies to foster innovation and coordinate data governance with clear objectives.
- In federal or highly decentralized countries, consider adapting data governance to subnational levels.

COLLABORATION AMONG STAKEHOLDERS:

- Promote collaboration between national governments and regional and international organizations to progress towards common goals.
- Encourage the involvement of various stakeholders, including developers, startups, academia, citizens, and others, to support governments in creating ecosystems.
- Stimulate citizen participation and digital education to enhance awareness of their rights, obligations, and responsibilities regarding the use of their data.

The **Health Data Governance Principles** emerge as a valuable tool to comprehensively address these mentioned challenges by promoting the development of an optimal ecosystem for innovation in AI in health, while keeping a focus on respecting human rights, ensuring people's safety, and promoting equity in healthcare systems.

GLOSARRY

AI: Artificial Intelligence

CJI: Inter-American Juridical Committee

CLIAS: Center for Artificial Intelligence in Health for Latin America and the Caribbean.

EBIA: the Brazilian Artificial Intelligence Strategy

ECLAC: Economic Commission for Latin America and the Caribbean

EHR: Electronic Health Records

EU: European Union

GCI: Global Cybersecurity Index.

GDPR: General Data Protection Regulation

IDB: Inter-American Development Bank

ITU: International Telecommunication Union

LAC: Latin America and the Caribbean

MERCOSUR: Southern Common Market

OAS: Organization of American States

OECD: Organization for Economic Co-operation and Development

PAHO: Pan American Health Organization

PB: Petabytes

R&D: Research and Development

RIPD: Ibero-American Data Protection Network

SDG: Sustainable Development Goals

T&E: Transparency and Explainability

UHC: Universal Health Coverage

UN: United Nations

UNCTAD: United Nations Conference on Trade and Development's

UNESCO: United Nations Educational, Scientific and Cultural Organization

WHO: World Health Organization

01. INTRODUCTION

This document aims to illustrate the current state and challenges faced by the Latin America and Caribbean (LAC) region regarding health data governance for the development of Artificial Intelligence (AI) solutions in this sector.

Significant technological advances in recent decades have opened up a broad horizon of possibilities and benefits due to the existence of vast amounts of personal data. This includes health data, as well as identification, contact, demographic, financial, and educational data, among other types. AI has already demonstrated not only its potential to transform healthcare systems and services but also its ability to enhance health through more accurate diagnoses, personalized treatments, and improvements in healthcare access through various innovative developments.

However, the existence of this crucial resource also entails the **need for principles, policies, regulations, and practices** that guide the efficient management of data to ensure responsible, secure, and rights-respecting treatment. This is crucial to improve the health of populations and individuals, avoiding the creation and deepening of existing gaps and preventing the reproduction of biases based on gender, language,

physical characteristics, and other potential sources of discrimination. **This is commonly referred to as "data governance."**

This document aims to address the **complex intersection between data governance and the implementation of AI developments in health in Latin America and the Caribbean (LAC)**. It considers **the existence of the Health Data Governance Principles**, providing a conceptual framework for addressing the challenges present in the region.

To achieve this, a literature search and review were conducted, along with five interviews involving seven experts and a webinar featuring specialized panelists in various areas related to AI, data governance, and digital health. As a result, the current scenario is explored to understand the existing tools that countries have for data governance and the protection of individuals' information. Additionally, the level of development in AI, both in general and in health specifically, is examined. The document identifies the primary challenges and obstacles that countries in the region face in these areas and, based on that analysis, proposes recommendations to enhance data governance and promote innovation.

02. HEALTH DATA GOVERNANCE: WHY DOES IT MATTER?

The widespread implementation of digital technologies is causing significant transformations across all industries, including the healthcare sector. In this process of change, **data emerges as a fundamental asset for any organization.**

The substantial technological advances of recent decades and the development of Artificial Intelligence (AI) in the healthcare domain have opened a horizon of benefits and potentialities that have already radically changed both research and medical care. Agility and precision in disease diagnosis and treatment, along with increased efficiency in healthcare, are just a few advantages that innovative tools can provide. AI has also contributed the ability to identify patterns and trends in extensive datasets, facilitating early disease detection and evidence-based decision-making. It enables personalized healthcare by adapting treatments and care precisely to the individual needs of each patient and generates innovative solutions to complex problems.

Health data serves as a fundamental input for these developments. Digitization has led to an exponential growth in the production and application of health-related data. It is estimated that a hospital can generate up to 50 petabytes (PB) per year (1 PB equals 500 billion pages of text)¹. **This vast availability of timely information brings notable advantages for healthcare professionals, policymakers, and citizens interested in improving both individual and public health.**

According to a report prepared in 2021 by the Economic Commission for Latin America and the Caribbean (ECLAC)², **the recognition of data as a critical component for decision-making has driven various**

initiatives at the governmental level, both nationally and regionally. Consequently, conceptual frameworks addressing key aspects for effective data governance in strategic and technical terms have been developed. These frameworks consider elements such as **data quality, interoperability, infrastructure, and security**, among others. In this direction, many governments have adopted national data strategies with the aim of promoting coherent public policies and maximizing the potential use of data, although the progress varies among countries and depends on local contexts.

Data governance has experienced some progress in Latin American governments over the last decade, although it still faces notable challenges in terms of access, use, data protection, and evidence-based policy design. While some countries stand out in data openness, **few have succeeded in establishing a data culture and developing a comprehensive data governance program.** Therefore, **it is necessary to foster greater awareness of the potential of data among decision-makers, citizens, and civil society to effectively integrate them into the public agenda².**

Managing data in the health sector presents significant peculiarities that pose challenges in handling and transforming it into useful information. One of the main challenges lies in **finding the delicate balance between ensuring data availability and maintaining its security, considering the inherent sensitivity of medical information.** Increased availability and openness of personal and health data can facilitate and promote significant improvements in healthcare and access to health services. However, this information is part of people's private and intimate lives, and its disclosure or use for purposes other than those for which it was collected

carries **the possibility of discrimination, stigmatization, and human rights violations.**

Unauthorized disclosure of sensitive data can lead to workplace discrimination, as an individual may not be hired based on their medical conditions. Additionally, a person could become a victim of blackmail or extortion, being threatened with the exposure of their health information. Moreover, this could have psychological consequences, such as anxiety or depression, for the affected individual.

Another challenge present in the generation and use of health data is related to its fragmentation. In many cases, individuals' health data is collected in separate silos, promoting duplications and multiple versions of the same information. Interoperability emerges as a crucial solution to bridge these silos, allowing for efficient data sharing, facilitating timely access, and ensuring data integrity.

The fragmentation of health data results in several problems, ranging from the inability to have an integrated medical history and healthcare professionals lacking a comprehensive view of patients' health to medical errors, duplication of diagnoses, and delays in result deliveries. Moreover, fragmented data poses challenges for innovation in AI, as this and other technologies require large amounts of high-quality data.

Moreover, **data aggregation**, which involves the need to combine and consolidate information from various sources, becomes the essential foundation for decision-making at all levels of healthcare management. The highest expression of this aggregation is the use of data to drive business intelligence and analytics, enabling informed and strategic decision-making. It is worth

noting that currently, 80% of generated information is unstructured,³ **and inadequate governance of health data could intensify disparities, perpetuate biases and discrimination against marginalized groups, and undermine human rights and people's health.**

The aggregated use of data allows, for example, the conduct of epidemiological analysis of diseases by obtaining valuable population-level information and conducting statistical analyses to identify trends and patterns. Having this information enables decision-makers to formulate evidence-based public policies.

What are the different ways in which poor health data governance can foster discrimination against individuals?

- **Biases in Data Collection:** for example, if a system only collects data from hospitals located in urban areas and excludes data from rural communities, a geographical bias is introduced in the data since health conditions and disease patterns may differ between the two areas.

- **Biases in Algorithms and Predictive Models:** for example, if an algorithm is trained to predict the risk of heart diseases using historically biased data towards the white population, the model may not accurately predict the risk in ethnic minority populations as it has not adequately learned from their diversity.

- **Lack of Transparency and Accountability:** for example, if an organization uses an algorithm to allocate medical resources but does not disclose how decisions are made and fails to provide a clear mechanism for patients to challenge decisions, this

can conceal biases and hinder the identification and correction of problems.

- Lack of Representation in Decision-Making: for example, if a data governance committee is primarily composed of healthcare professionals from a single specialty and lacks representation from minority communities, this can lead to decisions that do not fully consider the needs and perspectives of diverse groups.

- Inequalities in Access and Use of Technology: for example, if a health monitoring application relies on mobile devices, but those without access to smartphones or robust internet connections cannot use it, this creates a bias in the collected data by excluding those who may face inequalities in accessing technology.

These particularities illustrate the **complexity and importance of framing the use of health data within governance parameters that ensure the safety of individuals and their data, promote equitable access to healthcare, uphold ethical values, and protect human rights, especially in the context of the increasing application of artificial intelligence in global healthcare.** In LAC, the disparities within countries in healthcare access, internet accessibility, and technological development add complexity to the scenario.⁴

Data governance primarily involves a set of principles, policies, and practices aimed at ensuring efficient management of data for decision-making throughout its lifecycle to optimize the ability of an individual, organization, or government for political, strategic, and operational management.

Specifically in health, it refers to the process of management and decision-making to guide the generation, collection, storage, and management of health data through actionable, cross-cutting policies, practices, standards, benchmarks, and regulatory rules.⁵

New technologies are advancing more rapidly than the capacity of states to provide regulatory and public policy responses. While this poses a significant challenge, it **also presents opportunities for the development of regulations, policies, and agreements at the national and international levels** to protect residents, especially vulnerable populations and communities, while fostering digital transformation.

One of the most commonly used tools internationally is the so-called **"soft laws."** These legal instruments are non-binding norms, meaning they do not impose specific legal obligations and do not result in direct legal consequences for non-compliance. They often take the form of **declarations, resolutions, codes of conduct, principles, and guidelines, serving to provide guidance and standards of best practices in various areas, aiding in policy formulation and development, enhancing international coordination among countries, and being more flexible and adaptable to contexts than binding laws.** In dynamic and rapidly advancing technological environments, these instruments become more relevant and useful.

To guide countries toward **better data governance, digital health, and AI in LAC** and worldwide, various international organizations have utilized these resources. **Below are brief presentations of some of these regional or global initiatives.**

GLOBAL AND REGIONAL INITIATIVES

Within the international community, one of the key guiding resources for member states of the United Nations (UN) is the **Sustainable Development Goals (SDGs)**, which are part of the 2030 Agenda established by the UN in 2015. The SDGs define 17 areas in which countries have the opportunity to advance towards

economic development and address various social needs contributing to poverty eradication.⁶ **In this context, data governance in health, new technologies, the advancement of AI, and the importance of reducing inequalities and technological gaps to promote equity in both access to health services and access to these new technologies resonate with several of these goals.**

SDG 1: No poverty	It includes ensuring that all people, especially the poor and the most vulnerable, have equal rights to access economic resources, basic services, land ownership, and other assets, inheritance, natural resources, new technologies, and economic services.
SDG 3: Good health and well-being	Among its goals are achieving Universal Health Coverage (UHC) and the implementation of Digital Health strategies.
SDG 5: Gender equality	It emphasizes the importance of equitable access to technological advancements to promote the empowerment of women.
SDG 9: Industry, innovation and infrastructure	It includes among its goals supporting the development of technologies, research, and innovation nationally in developing countries and increasing access to information and communication technologies, including the Internet.
SDG 10: Reduced inequalities	It emphasizes the generation of regulations and public policies by states to reduce intersectional inequalities that affect populations in economic, social, and gender-related issues, among others.
SDG 16: Peace, justice and strong institutions	It establishes the need to create effective and transparent institutions that are accountable, ensure inclusive, participatory, and representative decision-making at all levels, expand and strengthen the participation of developing countries in global governance institutions, and ensure public access to information and protect freedoms in accordance with national laws and international agreements.

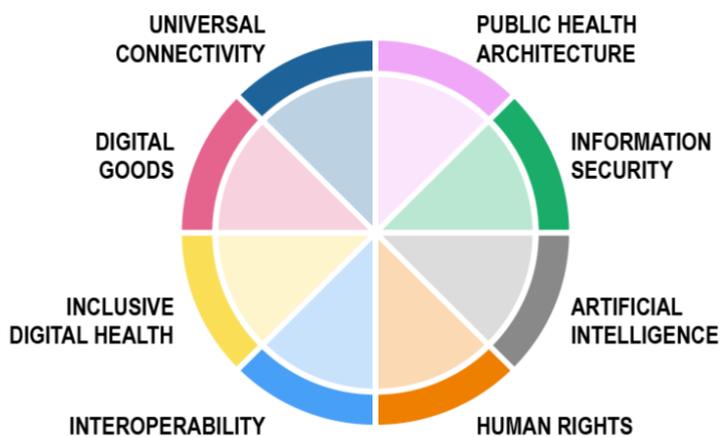
Source: Sustainable Development Goals, United Nations⁶

In this way, **the SDGs seek to pave the way for different states to advance policies and make decisions aimed at reducing existing gaps and disparities in access to health, technological**

development, and institutional guarantees for development that is not only sustainable but also equitable, leaving no one behind.

Likewise, as part of its 2019-2023 Plan of Action for Health Information Systems (IS4H), the Pan American Health Organization (PAHO/OPS) proposed 8 Principles for the **Digital Transformation of the Health Sector**. These principles aim to provide guidance to countries in

the region on digital transformation processes, enabling them to make informed decisions and formulate public policies in this area while emphasizing the pursuit of health equity.⁷



On the other hand, **concerning AI advancements**, various organizations such as the United Nations Educational, Scientific and Cultural Organization (UNESCO)⁸, the Organization for Economic Co-operation and Development (OECD)⁹, and the World

Health Organization (WHO)¹⁰ have developed frameworks, recommendations, principles, or guidelines to guide and promote the development of AI centered on respect for human rights, reliability, safety, and effectiveness

UNESCO: Recommendation on the Ethics of Artificial Intelligence

4 fundamental values:

- Human Rights and human dignity
- Living in peaceful societies
- Ensuring diversity and inclusion
- Flourishing of the environment and ecosystems

10 basic principles:

- Proportionality and harmlessness
- Security and protection to prevent potential harm
- Right to privacy and data protection
- Governance and collaboration of stakeholders
- Responsibility and accountability



	<ul style="list-style-type: none"> ○ Transparency and Explainability (T&E) ○ Oversight and human decision-making ○ Sustainability ○ Awareness and education Equity and non-discrimination
<p>OECD: Principles to Promote the Use of AI within the Framework of Human Rights and Democracy⁹</p>	<p>Principles aimed at promoting the use of AI in an innovative and reliable manner, within the framework of respect for human rights and democracy:</p> <ul style="list-style-type: none"> ○ Inclusive Growth ○ Sustainable Development and Well-being ○ Human-Centered Values and Equity ○ Transparency and Explainability (T&E) ○ Robustness ○ Safety and Protection ○ Accountability <p>Principles aimed at providing recommendations to policymakers:</p> <ul style="list-style-type: none"> ○ Invest in research and development (R&D) in AI ○ Foster a digital ecosystem for AI ○ Create a conducive political environment for AI ○ Develop human capability and prepare for the transformation of the labor market ○ International cooperation for reliable AI.
<p>WHO: Regulatory Considerations on AI for Health¹⁰</p>	<p>Six areas for AI regulation:</p> <ul style="list-style-type: none"> ○ Transparency and documentation ○ Risk management and clarity on the intended use of data ○ Data quality ○ External validation of data ○ Privacy and data protection ○ Encouraging collaboration among different stakeholders
<p>Khipu – Latin American AI Summit: Montevideo Declaration on AI and Its Impact in Latin America¹¹</p>	<p>Technologies, especially AI, should:</p> <ul style="list-style-type: none"> ○ Benefit people, prioritizing the improvement of quality of life, economic conditions, health, and general well-being. ○ Comply with Human Rights, avoiding the perpetuation of stereotypes or exacerbation of inequality. ○ Not cause harm to individuals and minimize environmental impact. ○ Evaluate and mitigate risks from the design phase.

- Respect cultural diversity in the design and training of AI models to avoid the exclusion of Latin American perspectives.
- Involve populations.
- Strengthen the sovereignty of Latin American countries in strategic and regulatory issues related to AI.

These different principles or standards demonstrate that there is a **shared interest on the part of the international community in promoting AI in accordance with certain basic tenets, such as respect for human rights, the safety of individuals and their data, transparency and accountability, cooperation, and the prevention of discrimination or the reproduction of inequalities.**

Regarding the **protection of health data and any type of personal data of individuals and communities**, this need has also been addressed by different transnational organizations. The most prominent

initiatives include the Council of Europe's **Convention 108**, titled "**Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**" the **General Data Protection Regulation (GDPR)** of the European Union (EU)¹², the "**Data Protection Standards of Ibero-American States**" of the **Ibero-American Data Protection Network (RIPD)**¹³, and the **Updated Principles on Privacy and the Protection of Personal Data** adopted by the **Inter-American Juridical Committee (CJI)** and approved by the **General Assembly of the Organization of American States (OAS)**.

**Council of Europe's
 Convention 108: "Convention
 for the Protection of
 Individuals with regard to
 Automatic Processing of
 Personal Data"**

- Understands personal data as any information related to an identified or identifiable person.
- Ensures the protection of the fundamental rights and freedoms of individuals with respect to that data.
- Establishes that data should be collected fairly and lawfully, and that it should be adequate and relevant.
- Recognizes individuals' rights regarding their data: access, rectification, opposition.
- Facilitates cross-border data transfers.
- Sets requirements for security and confidentiality.
- Encourages the establishment of independent supervisory authorities.
- Requires notification of security breaches.
- Recognizes the right to compensation for the unlawful use or processing of data.

**EU: General Data Protection
 Regulation (GDPR)**

- Establishes the extraterritorial scope of application.
- Sets principles for data processing: legality, fairness, transparency, purpose limitation, and data minimization.
- Reinforces the need for informed consent.

	<ul style="list-style-type: none"> ○ Recognizes individuals' rights as data subjects: access, rectification, erasure, portability, and objection. ○ Mandates the obligation to notify data breaches. ○ Encourages the appointment of a data protection officer. ○ Recommends data protection impact assessments. ○ Regulates international data transfers. ○ Imposes sanctions and fines.
<p>RIPD: Data Protection Standards of Ibero-American States</p>	<p>Principles for data protection:</p> <ul style="list-style-type: none"> ○ Legitimacy ○ Lawfulness ○ Transparency ○ Loyalty ○ Purpose ○ Proportionality ○ Quality ○ Responsibility ○ Security ○ Confidentiality ○ Responsibility of data processors ○ Rights of data subjects: access, rectification, erasure, objection, and portability.
<p>OAS: Updated Principles on Privacy and the Protection of Personal Data</p>	<p>Principles for the use of personal data:</p> <ul style="list-style-type: none"> ○ Legitimate purposes and loyalty ○ Transparency and consent ○ Relevance and necessity ○ Limited processing and retention ○ Confidentiality ○ Responsibility ○ Security ○ Data accuracy ○ Rights of data subjects: access, rectification, erasure, objection, and portability ○ Consideration of sensitive personal data ○ Cross-border flow of data

All these initiatives share common points regarding the parameters that should guide the protection of people's data, establishing the rights of data

subjects, the flow of data between countries, the need to develop security measures, and the importance of fair and responsible data processing.

It is clear, then, that **the need to strengthen the governance of health data is a current issue on the global agenda and in the LAC region.** The significant progress of technologies requires a set of accepted principles for managing this data, reflecting regional and sectoral diversity, with the purpose of correcting the unequal distribution of benefits and harms resulting from the collection, analysis, and use of this sensitive data. **An approach that allows for strengthening and promoting innovation without leaving anyone behind is, therefore, a necessary tool for the challenges of the present and the future.**

WHAT ARE THE HEALTH DATA GOVERNANCE PRINCIPLES?

In this scenario, the Transform Health Coalition, along with numerous experts in the field of digital health, developed the **Health Data Governance Principles** with the aim of providing a human rights and equity perspective to the use of health data. The goal is to contribute to the construction of resilient and sustainable

health systems that advance towards Universal Health Coverage (UHC)¹⁴.

These principles seek to **contribute to the creation of a global framework for health data governance that can support the use of technologies and digital data for the collective well-being.** They were designed and promoted by civil society through an inclusive and consultative process, incorporating a wide variety of perspectives and knowledge from different geographical regions, sectors, and stakeholders to guide governments, technology companies, and other entities involved in the collection and use of health data. Additionally, they are considered an essential tool for organizations advocating for an equitable governance of health data based on human rights. **In this sense, the Principles are regarded as a public good, available to be incorporated into political work, policy design, and the advocacy for health data governance.**

The Principles are organized around three fundamental axes: **Protect people, promote health value, and prioritize equity.**

PROTECT PEOPLE	PROMOTE HEALTH VALUE	PRIORITIZE EQUITY
Protect individuals and communities	Enhance health systems and services	Promote equitable benefits from health data
Address individual and collective risk	Evaluate the benefits of health data	Represent all groups and populations equitably in data
Collect data with defined purposes	Use data to enhance health services for individuals and communities	Consider the unique needs of marginalized groups and populations
Collect personal or sensitive data only when necessary and with informed consent	Encourage a culture of data-led insights and action	Mitigate data bias

CHALLENGES AND RECOMMENDATIONS IN DATA GOVERNANCE
**FOR THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE
 IN HEALTH IN LATIN AMERICA AND THE CARIBBEAN**

Use secure data collection and storage mechanisms	Address health system efficiency, effectiveness, and resilience	Use accessible language and plug knowledge gaps
Use de-identification and anonymization	Strengthen community ownership of health data	Implement inclusive data feedback mechanisms
Define inappropriate uses of health data	Enable and empower frontline health workers	Promote equitable impact and benefit
Institute safeguards against discrimination, stigma, harassment and bias	Promote data sharing and interoperability	Establish data rights and ownership
Provide guidance specific to marginalized groups and populations	Establish data sharing rules and guidelines	Apply a human rights lens to health data governance
Built trust in data systems	Validate informed consent before sharing data	Define clear governance roles and responsibilities
Align with best practices for data protection and privacy	Promote interoperability of data systems	Codify data rights and ownership
Ensure consent is informed and understood in all its complexities	Define common data structures across health systems	Extend data rights and ownership to products and services
Obtain collective consent where appropriate	Define multiple levels of data access	Develop health data trusts and health data cooperatives
Define concrete exceptions to informed consent	Use common definitions and global standards	Employ participatory data governance mechanisms
Ensure data quality, availability, and accessibility	Support multi-sector partnerships	Connect to broader accountability mechanisms
Reinforce health data governance with evidence	Facilitate innovation using health data	

Establish transparent and accessible processes and systems	Apply health data governance to emerging technologies	
Institute feedback and accountability mechanisms	Address the use of non-health data in health contexts	
Ensure data security	Build public health data infrastructure	
Require strong technical security measures for data processing	Employ policy innovation	
Mitigate risks related to security threats		
Ensure transparency around data breaches		
Consider federated data systems		

Source: *Transform Health*¹⁴

The first axis, "**Protect people**" aims to establish that health data governance must ensure the safeguarding of individuals, groups, and communities against the potential threat of harm or violations in the use of their data. While the protection of individuals is generally addressed in data protection laws, the sensitivity of health data requires additional specialized safeguards in both the legal framework and data management practices. The absence of health data protection, whether individual or aggregated, could expose individuals, groups, and communities to risks. Specific

protection measures against various types of harm, such as exploitation, harassment, discrimination, commercial surveillance, and data-driven neocolonialism, must be implemented in health data governance.

In this regard, the principles included in this axis **focus on the protection of individuals and communities, the need to build trust in data systems, and ensuring data security.**

IN WHAT CASES CAN THE MISUSE OF HEALTH DATA PUT INDIVIDUALS AND COMMUNITIES AT RISK, AND WHY IS IT NECESSARY TO PROTECT THEM?

Unauthorized access to data	An employee at a hospital accessing a patient's medical records without a legitimate reason or authorization.
Sale of medical information	A clinic selling health information of its patients to a marketing company without the knowledge or consent of the patients.
Improper access to electronic records	A hacker breaching the security of an electronic medical records system to access and modify information.
Discrimination based on personal data	An employer using medical information of job candidates to make hiring decisions, excluding those with specific health conditions or belonging to a particular community.

SOME EXAMPLES OF BEST PRACTICES THAT HIGHLIGHT THE IMPORTANCE OF BUILDING TRUST IN DATA SYSTEMS

Transparency in data collection and use	A healthcare service provider that communicates clearly and comprehensibly how patient data is collected and used, providing detailed information to patients.
Clear and comprehensible informed consent	A hospital implementing a process for obtaining informed consent that explains in detail the purposes of the treatment, the duration of consent, and offers clear options for patients to exert control over their information.
Compliance with data privacy regulations and standards	A healthcare organization that strictly adheres to privacy regulations, such as GDPR or local regulations, and builds trust by ensuring ethical and legal practices in handling personal data.

WHAT MEASURES CAN BE IMPLEMENTED TO ENSURE DATA SECURITY?

Implementation of robust data security measures	<p>Una institución de salud puede invertir en medidas de seguridad de datos avanzadas, como cifrado, autenticación de dos factores y protocolos de acceso seguro.</p>
Effective response to data breaches	<p>En caso de una violación de datos, una organización de salud debe responder de manera rápida y transparente: informar a los afectados, tomar medidas correctivas y ajustar sus prácticas para evitar futuras violaciones.</p>
Education on security and privacy	<p>Los proveedores de salud pueden educar a los pacientes sobre la importancia de la privacidad y la seguridad de los datos a través de materiales informativos, capacitación y recursos para empoderar a los individuos en la comprensión de cómo se manejan y protegen sus datos</p>

The second axis, "**Promote Health Value**" focuses on the idea that promoting the value of health data involves optimizing its management to enhance healthcare at both individual and societal levels. Furthermore, as data-driven approaches can lead to innovative medical services, health data governance should support and

stimulate such innovations. In this context, the principles included in this axis center around three overarching general principles: **Enhance health systems, promote data sharing and interoperability, and facilitate innovation using health data.**

HOW CAN DATA GOVERNANCE CONTRIBUTE TO IMPROVING HEALTHCARE SYSTEMS AND CONTRIBUTE TO UHC?

Data analysis to prevent diseases	<p>If data from various sources, such as medical records, health surveys, and socioeconomic factors, are collected, they can be analyzed to identify patterns and trends that may predict disease outbreaks in specific communities. This allows for more effective preventive interventions and public health strategies.</p>
Monitoring healthcare inequalities	<p>Specific indicators can be incorporated to assess inequalities in access and quality of healthcare. Continuous monitoring of these indicators helps identify disparities and address systematic issues affecting marginalized communities, promoting equity in healthcare.</p>
Community involvement in decision-making	<p>Governance can involve the community in decision-making regarding health policies. This ensures that the needs and perspectives of different groups are considered, contributing to a more equitable approach in resource allocation and service planning.</p>

WHY IS IT IMPORTANT TO PROMOTE DATA EXCHANGE AND INTEROPERABILITY?

Establishing interoperable standards for sharing data among different health systems and organizations enhances collaboration, reduces communication errors, and facilitates the transition of patients between different providers, improving the continuity of care.

HOW CAN HEALTH DATA MANAGEMENT FACILITATE INNOVATION?

Effective data governance enables access to large datasets for model development in an ethical and secure manner. This facilitates researchers and AI developers to use diverse data, representative of different communities, to train robust and accurate models. For instance, a predictive model for early detection of cardiovascular diseases can be developed, serving as support for decision-making in public health policies for diverse populations.

Finally, the third axis, "**Prioritize Equity**", focuses on the idea that the value derived from the use of data should be distributed fairly for the benefit of both individuals and communities. It emphasizes that those who contribute their data should have an equitable

share in the health benefits generated by their data. This axis includes two overarching general principles: **Promote equitable benefits and establish data rights and ownership.**

HOW CAN EQUITABLE BENEFITS FROM DATA BE PROMOTED THROUGH THEIR GOVERNANCE?

Equitable access to health technologies	Policies can be implemented to ensure equitable access to health technologies, such as telemedicine. This is particularly crucial for rural or marginalized communities that may face challenges in accessing traditional healthcare.
Cultural and linguistic adaptability	By promoting culturally and linguistically sensitive health information systems, including the translation of materials and adaptation of platforms to be accessible to individuals from different cultural and linguistic backgrounds.
Inclusion of socioeconomic data	Integrating socioeconomic data into governance to better understand the social determinants of health, allowing for more effective intervention in issues such as homelessness, unemployment, and other factors that may disproportionately affect health in certain groups.

<p>Health education and literacy</p>	<p>Developing health education and literacy programs that address barriers in understanding health information. This is crucial to ensure that all individuals, regardless of their level of education, can fully benefit from available health information.</p>
---	--

VARIOUS MEASURES THAT CAN BE TAKEN TO ESTABLISH DATA OWNERSHIP RIGHTS:

<p>Participatory data governance mechanisms</p>	<p>Participatory decision-making mechanisms can be implemented to involve the community in decisions related to the collection and use of health data. This may include community ethics committees or citizen engagement forums that enable active input from individuals in shaping data policies.</p>
<p>Clear definition of roles and responsibilities</p>	<p>Clear policies and regulations can be established to define the functions and responsibilities of each entity involved in health data management. This may include specific roles for healthcare providers, research institutions, health authorities, and individuals themselves, ensuring a transparent and ethical division of responsibilities</p>
<p>Development of health data trusts or cooperatives</p>	<p>Health data trusts or cooperatives can be established to act as independent custodians of information. These entities can be managed by representatives from communities, healthcare professionals, and ethics experts, with their primary function being to safeguard the interests and rights of individuals who own the data.</p>

03. HEALTH DATA GOVERNANCE AND AI IN LATIN AMERICA AND THE CARIBBEAN

WHAT IS THE SCENARIO IN THE REGION?

The governance of individuals' health data is, therefore, one of the most important aspects to consider when developing AI solutions and other innovative technologies in this field. **While AI holds significant potential to contribute to improving health and access to healthcare services, the handling of personal and sensitive patient data requires measures, standards, and policies aimed at providing protection and security.**

In this context, **the LAC region faces significant challenges in the implementation of policies and measures regarding the governance of personal data in health, the development of AI strategies, as well as the security and cybersecurity of data.**

In 2020, the Inter-American Development Bank (IDB) conducted a mapping of regulations on health data for the use of Electronic Health Records (EHR), Telemedicine, and Digital Health Strategies in Latin America and the Caribbean. According to this study, the 24 countries in the region covered exhibit varying degrees of regulatory development concerning the protection of individuals' data, secondary use of health information, patients' role in relation to their health data, and the use of standards for EHR use and interoperability. Details are available in the Annex.

While the majority of countries have regulations and public policies addressing the protection of personal data, patient rights, health system obligations, and

access to public information, **most of these rules do not comprehensively address the requirements associated with the development of new technologies and the vast amounts of data, and they are outdated.** It is also noteworthy that concerning standards for EHR use and interoperability, the regional average of countries that have developed and implemented regulations or policies on this matter is less than 50%.

On the other hand, in 2023, the Economic Commission for Latin America and the Caribbean (ECLAC) has produced a document on **the state of regulatory frameworks regarding cybersecurity**, which is a fundamental aspect to consider when contemplating the governance and protection of health data in a context of extensive digitized data¹⁵.

According to this report, **the region has seen progress in strengthening regulatory frameworks related to data protection and cybersecurity. However, not all countries in Latin America and the Caribbean have regulatory tools in these areas.** According to the United Nations Conference on Trade and Development's (UNCTAD) Global Cyberlaw Tracker, **only 24 out of the 33 countries in the region have specific legislation on privacy and the protection of personal data.** Regarding data security, the International Telecommunication Union's (ITU) Global Cybersecurity Index (GCI) **reveals significant disparities among the countries in the region.** Brazil leads the ranking with 96.6 points out of 100, followed by Mexico, Uruguay, and the Dominican Republic, all with scores above 75. In contrast, some countries in

Central America and the Caribbean score below 15 points.

In this sense, **greater alignment of regulatory frameworks in the region regarding data protection and cybersecurity could yield significant economic and social benefits. This includes increasing the trust of both domestic and foreign investors, stimulating innovation, diversifying the economy, and facilitating scalability.** In this context, interoperability is directly linked to public policies, as countries must promote not only technical and legal compatibility between different systems but also strengthen international cooperation to facilitate, for example, the secure transfer of data across borders.

How can regional alignment of regulatory frameworks contribute to promoting innovation while improving data protection and cybersecurity?

The implementation of the **General Data Protection Regulation (GDPR)** in the EU in 2018 served as an example of regulatory alignment. This regulation established a common standard for data protection across the region, not only **strengthening the privacy of European citizens but also simplifying the regulatory environment for businesses by eliminating the need to comply with different regulations in each member country.** This led to increased consumer trust and facilitated cross-border business operations.

On the other hand, global companies like Google, Facebook, and others must comply with a variety of privacy and security regulations in different countries. When unified standards exist, these companies can **optimize their processes and**

resources, rather than having to adapt to diverse regulations in each country where they operate. This reduces operational costs and allows them to focus more on innovation and product development.

In the healthcare sector, specifically, the need for modification of cyber defense strategies by states becomes imperative, as it is one of the sectors that has received the most attacks, along with education, research, and the government sector. For example, recent experiences in Argentina and Colombia are notable, where **serious cyberattacks targeted the portals of their Ministries of Health, putting the health data of millions of people at risk.**^{16,17}

Another report by ECLAC in 2021 on the state of cybersecurity maturity in Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, the Dominican Republic, and Uruguay establishes that, **despite a significant increase in awareness of cybersecurity and its relevance in the analyzed countries, regulatory and legislative updating activity is scarce or even nonexistent.** Among these analyzed countries, only Colombia shows substantial and concrete progress by introducing five new national decrees, followed by Chile and Ecuador, which made significant regulatory updates.¹⁸

Different countries have made progress, albeit uneven, in **regulating aspects related to the use of individuals' personal data, health data, digital health, and AI.** As mentioned in the section "*Health Data Governance, why does it matter?*" technological development has increased awareness of the need for the protection of personal data, EHRs, and patient rights. This has led, albeit heterogeneously among countries, to updates or new regulations and public policies aimed at safeguarding patient information and the secondary use of their data. It also aims to guide

healthcare services and systems in information security, as well as in the search for tools for data use that enable innovation, research, management control, evaluation, and planning.

According to the Governant AI Readiness Index,²⁰ developed to assess technological readiness, and despite the inclusion of startups and investment in

technology and health governance due to the COVID-19 pandemic, the **governmental readiness for AI among countries in LAC is uneven. The technological sector still struggles to be competitive in the region. Out of the twelve countries analyzed, only two have an AI strategy, five are exploring its development, and the rest do not have an explicit artificial intelligence strategy.**

	Digital strategy	Data strategy	AI strategy	Infrastructure and conectivity
Argentina	Yes	Yes	For exploring continuity	Very advanced
Brazil	Yes	Yes	On going	Very advanced
Chile	Yes	Yes	On going	Lider
Colombia	Yes	Yes	Yes	Very advanced
Costa Rica	Yes	Yes	On going	Very advanced
Dominican Republic	Yes	Yes	No	Semi advanced
Ecuador	Yes	Yes	No	Semi advanced
Mexico	Yes	Yes	For exploring continuity	Advanced
Paraguay	Yes	Yes	No	Semi advanced
Peru	Yes	Yes	No	Advanced
Trinidad and Tobago	Yes	No	No	Advanced
Uruguay	Yes	Yes	Yes	Lider

Source: Self-developed based on “Artificial Intelligence in the Service of Social Good in Latin America and the Caribbean: Regional Overview and Snapshots of Twelve Countries” IDB - CMINDS²¹

Among the countries that have developed a strategy or national policy plan for the use of AI or are in the process of doing so, Colombia, Chile, Brazil, and Uruguay stand out. In these cases, it is also worth noting the aspects they consider regarding data governance.

In the **National Artificial Intelligence Plan of Colombia**,²² specific strategies for data governance are proposed, such as the creation of test environments ('sandbox') to encourage innovation in regulated sectors

such as Fintech, Healthtech, Agritech, and Govtech. There is also a plan to establish data infrastructure, focusing on the exploitation of public and market data, and efforts will be made to implement measures for responsible information management, including defining guidelines for Data Trusts or Data Commons, along with the necessary regulation. This focus on data governance is crucial to ensure controlled development of AI, assessing its impacts on various markets, and contributing to sustainable development and innovation



in the country. Additionally, an AI Task Force has been established with the aim of strengthening commitment and credibility in the formulation of public policies in artificial intelligence.

On the other hand, the **AI strategy in Chile**²³ focuses on the availability and quality of data, promoting an ecosystem of open and secure data that respects people's rights. It emphasizes the importance of trust, accurate representation of reality, quality, bias reduction, interoperability, and data security. The strategy proposes the creation of Natural Laboratories to develop repositories of high-quality data. Additionally, it seeks to update regulations on the use of personal data to ensure privacy and prevent arbitrary discrimination, following international standards such as GDPR. To achieve these objectives, the strategy proposes maintaining updated regulations, establishing data governance in the government, promoting public-private collaboration, encouraging anonymization and computational security technologies, promoting the availability of scientific data, and facilitating the creation of user communities.

Similarly, the **Brazilian Artificial Intelligence Strategy (EBIA)**²⁴ prioritizes the protection of personal data, the prevention of discrimination and algorithmic bias, and seeks a balance to foster the development of AI within legal parameters and responsibility. It aligns with Brazil's General Data Protection Law and emphasizes transparency and explainability to address discrimination. The EBIA also advocates for establishing legal parameters for legal certainty and relies on initiatives such as e-Digital, Startup Brazil, and the proposal to create a National Center for Artificial Intelligence to promote collaboration and ethical

treatment of AI.

Finally, Uruguay's AI Strategy²⁵ emerges as a tool to enhance e-government and aims to boost human capabilities to improve the quality of life. With a focus on the general interest, it seeks to ensure inclusion and equity, reducing unwanted biases. It highlights respect for human rights, transparency in the use of AI in public administration, and emphasizes addressing ethical dilemmas humanely. Additionally, it emphasizes the importance of privacy by design and requires compliance with basic information security principles according to current regulations in Uruguay.

At the regional level, there are also initiatives in this direction, such as **fAIr LAC, the Alliance for Ethics, Equity, and Transparency in Artificial Intelligence in Latin America and the Caribbean**. Its main objective is to promote ethical use of AI in the region. To achieve this, a strategy has been designed based on **three dimensions**. The first involves **creating a diverse network of AI experts to advise on policy development and action lines**. The second dimension focuses on **capacity building, aiming for policymakers, citizens, and businesses to understand the challenges and possibilities of AI**. Finally, the third dimension **promotes quality and risk mitigation through guidelines, self-regulation, quality standards, and regulatory frameworks**. These strategies are intended to be implemented at both the regional and territorial levels, with local hubs acting as references to promote ethical and equitable AI in their geographical areas. Feedback and learning between the regional initiative and local hubs will be essential for generating knowledge and best practices throughout the region.²⁶

WHAT ASPECTS OF DATA GOVERNANCE SHOULD BE CONSIDERED AT EACH STAGE OF THE LIFECYCLE OF HEALTH DATA IN THE DEVELOPMENT OF AI SOLUTIONS?

STAGE OF GENERATION AND CAPTURE OF HEALTH DATA	STAGE OF STORAGE OF HEALTH DATA	STAGE OF DATA ACCESS AND SHARING	DATA DELETION STAGE
<p>The AI requires high-quality, accurate, and complete data for its training. These data are obtained from clinical practice: electronic health records, laboratory data, complementary tests such as X-rays or magnetic resonance imaging, epidemiological data from surveillance systems, censuses, health surveys, and records from medical, administrative, and pharmacy insurance, among others.</p> <p>Data governance allows the establishment of standards on which the collection and recording of comprehensive and quality data should be based, from such diverse sources</p>	<p>The AI needs efficient access to large datasets, which requires proper management of databases and secure, reliable storage systems.</p> <p>Data governance must contribute to establishing security and privacy policies to protect sensitive information and ensure confidentiality and the rights of individuals.</p>	<p>Protocols for interoperability and privacy must be established, allowing data to be shared securely, and patients to provide their informed consent</p>	<p>Secure deletion procedures must be established, and data retention should be regulated</p>

The governance of health data thus plays a central role in the development of AI solutions in healthcare, as not only an adequate amount of **data is required, but also that these data are of high quality, representative of the different communities that make up a society, and available securely and interoperably.**

Furthermore, there is a clear need throughout the region to intensify efforts to support both public and private institutions through updated and relevant regulations and policies that foster innovation and protect individuals.

WHAT ARE THE MAIN CHALLENGES?

The preceding sections leave open questions but also a certainty: the challenges that LAC faces in terms of data governance and the promotion of innovation and development in AI are numerous.

In addition to a bibliographic analysis of secondary sources, various experts were interviewed for the preparation of this document **to delve into the challenges and needs in data governance in the face of AI developments, current best practices, steps to follow, and how the Health Data Governance Principles can contribute to addressing these challenges.** A webinar was also conducted with regional experts in these areas, engaging in discussions on these topics. **The aim was to gather opinions from individuals belonging to various fields and countries in the region: experts in open data, research and development of AI solutions in health, health law and AI, and digital health.**

This process of information analysis and interaction with experts allowed the **consolidation of the main challenges and identified needs, which can be grouped into regulatory challenges, data quality challenges, state capacity challenges, infrastructure challenges, and challenges related to coordination among stakeholders.**

REGULATORY

One of the main challenges facing LAC region is the **deficient regulatory and normative development that serves as a framework for technological innovation in health. The pace of data generation and AI development is outpacing the ability of state structures to cope with it.** As analyzed in previous sections, current regulations on personal data in the

majority of countries in the region are general and lack a specific perspective on health data, resulting in a state of vulnerability for this data. This translates into low enforcement capacity through control structures and governance of these technologies, with potential risks of discrimination, especially in marginalized communities.

For this reason, it is crucial for states to advance in the development of clear, updated, and reliable regulatory frameworks that take into account the regional and local context and needs. These frameworks should promote innovation and development while striking a balance between access to information and the protection and privacy of individuals.

DATA QUALITY

Another major challenge facing the LAC in the development of AI solutions is **the low quality of available data. This poses problems for proper data governance as well.**

According to various experts, **data repositories in ALC are scarce and poorly representative of the diverse populations in the region.** In many cases, AI developments are based on "imported" algorithms generated with profiles mainly from European or North American countries, which do not reflect the context and diversity present in Latin American countries. Additionally, **public databases in the region are often outdated,** with annotations or low-quality images, introducing new biases and not guaranteeing that the information is complete and accurate.

Another challenge related to data quality in the region is **the lack of training for those involved in data collection, labeling, or any stage of data use.** Therefore, it is crucial for those working with databases, including healthcare professionals, to receive education in this regard.

These challenges underscore an urgent need: **it is essential that AI tools in health incorporate good practices and an ethical perspective from their early stages and throughout their development and implementation.** This ensures that the use of data in AI benefits humans, promotes health, and avoids harmful actions, discrimination, or injustice²⁷.

INFRASTRUCTURE

The LAC region also **faces challenges related to infrastructure for data access.** Promoting innovation cannot be done responsibly without the necessary infrastructure conditions, ensuring **not only access to the internet, electricity, or cloud space (which are not always guaranteed) but also guarantees regarding data security.** In this regard, **cybersecurity is one of the critical points to consider.** Measures against cybercrime need to be taken from governance, as the healthcare sector has been one of the most targeted.

It is important to note that these aspects, while fundamental, are not exclusive to the healthcare sector. **Finding solutions to these problems must be multidisciplinary, comprehensive, holistic, and should incorporate successful experiences from other sectors that have already made progress in this direction.**

STATES CAPACITY

Another central challenge in the region is **the capacity of states to effectively guarantee the protection of individuals' rights while promoting innovation in AI.**

Currently, states in the region largely **lack the capacity for the implementation and control of such policies.** **Bureaucracies and agencies specialized in data use are often lacking, and in most cases, the necessary**

profiles and/or government agencies are absent. It is essential to **promote the existence of specialized agencies in data use, privacy, and access to information, with experts in health data.**

This also translates into a lack of clear guidelines for the path that developers of AI applications and solutions in health should follow: which government institutions to turn to, which regulatory agencies are involved, and what requirements they must meet. **Unifying criteria through guidelines, manuals, or best practice guides that include ethical aspects can pave the way for advancing innovation while ensuring data security.**

As mentioned earlier, few countries in Latin America have national plans for digital health and AI. There is a need to **promote these strategies, including funding, education, ecosystem stimulation, and investment.** This also implies the need for discussions on AI implementation in health to include defining the priorities of healthcare systems from a strategic and organized perspective. It is important to **consider the internal organizational structure of states.** Federal and non-federal countries have different capacities for action due to their centralization or decentralization characteristics. In federal countries like Argentina, Brazil, or Mexico, this must also be addressed at the subnational level.

COLLABORATION AMONG STAKEHOLDERS

Better data governance in the context of AI also requires the **coordination of different actors involved in the processes.** Currently, despite the regional initiatives mentioned in previous sections, **countries in LAC can move towards greater coordination among them in defining common parameters for the use and exchange of data.** At the local and regional levels, participation from developers, startups, academia, and governments in creating and designing ecosystems

should be encouraged. **The goal is to involve the maximum number of stakeholders in finding solutions to national problems.**

Furthermore, **it is necessary to stimulate citizen participation and digital culture**, making them part of discussions about data use, empowering them with information to increase awareness of their rights, obligations, and responsibilities regarding data. In this regard, increased digital education and awareness of

the value of digital data are essential.

WHAT DO WE RECOMMEND?

From the challenges presented **and based on the analyzed Health Data Governance Principles, recommendations can be made for countries in LAC to move towards seeking AI solutions that protect people, prioritize equity, and promote health**

<p>Regulatory</p>	<ul style="list-style-type: none"> ○ Establish comprehensive, clear, up-to-date, and reliable regulatory frameworks on data governance to ensure both data protection and the promotion of innovation. These frameworks should include specific provisions for addressing and safely using health data. ○ Regulations should anticipate the protection of data against aggregation for the creation of population profiles. ○ Integrate health data governance at various levels of the healthcare system, including government, hospitals, care centers, universities, and any related entities.
<p>Data quality</p>	<ul style="list-style-type: none"> ○ Encourage the collection and use of local data that align with the context of the countries in the region and the demographic and epidemiological profiles to generate higher-quality solutions that are more representative of local populations. ○ Aim for the reduction and control of biases throughout the development of AI projects. ○ Incentivize the creation of updated public databases with complete and quality data. ○ Provide training for individuals working with data at any stage of the data cycle to ensure data quality is preserved. ○ Integrate elements of data use and management into the educational curricula of healthcare professionals in training.
<p>Ethical</p>	<ul style="list-style-type: none"> ○ Address ethical considerations from the early stages of project design to implementation and monitoring. ○ Involve experts in ethics and other relevant disciplines from the beginning of projects to mitigate biases. ○ Strive for the anonymization of health data, secure data hosting, as well as temporary and compartmentalized archiving of data. ○ Collect data with a specific research question or purpose.

CHALLENGES AND RECOMMENDATIONS IN DATA GOVERNANCE FOR THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE IN HEALTH IN LATIN AMERICA AND THE CARIBBEAN

<p>Infrastructure</p>	<ul style="list-style-type: none"> ○ Encourage domestic and foreign investment in digital infrastructure. ○ Design comprehensive cybersecurity plans that involve experts from various disciplines to achieve a holistic approach, including the healthcare sector.
<p>States capacities</p>	<ul style="list-style-type: none"> ○ Promote the existence of specialized agencies for data use and protection, privacy, and access to information, ensuring that these agencies have experts in health data. ○ Encourage the formation of a specialized state bureaucracy in data use and health data. ○ Develop manuals, guidelines, or best practice guides to inform developers of AI applications in health about the government processes they should follow for developing an AI health solution. ○ Advocate for the design and implementation of National Digital Health Strategies to foster innovation and coordinate data governance with clear objectives. ○ In federal or more decentralized countries, consider adapting data governance to subnational levels.
<p>Collaboration among stakeholders</p>	<ul style="list-style-type: none"> ○ Promote coordination between national states and regional and international organizations to work towards common goals. ○ Encourage the participation of different actors, including developers, startups, academia, citizens, and others, to support governments in creating ecosystems. ○ Stimulate citizen participation and digital education to raise awareness about their rights, obligations, and responsibilities regarding the use of their data.

04. CONCLUSIONS

The development of AI and other innovative technologies holds enormous potential to improve the health of people in LAC. However, this development cannot proceed without a policy of governance for health data.

The region faces numerous challenges in ensuring the protection of individuals' health data and security at all stages of the data processing process. The lack of appropriate regulatory frameworks and clear, coordinated strategies for AI development among the countries in the region, along with the low quality of available data and a deficit in awareness of the importance of responsible data use, pose risks but also significant opportunities. Comprehensive, coordinated responses based on the protection of individuals, their rights, and the promotion of human rights can address these challenges.

Technological advancements move faster than the capacity of states to provide immediate responses. For

this reason, institutions must be dynamic and resilient, creating broad regulatory frameworks that allow all stakeholders to adapt more effectively to exponential changes and make informed decisions to ensure that AI benefits society as a whole. It is crucial to protect and respect ethical principles, privacy, and equity in healthcare. In this context, the creation of digital public goods and adequate representation of populations are essential to ensure the promotion of equity and the protection of individuals. Universal connectivity is crucial to avoid underrepresentation and biased solutions that deepen existing gaps, foster discrimination, and violate people's rights.

Therefore, the Health Data Governance Principles emerge as a valuable tool to comprehensively address regulatory, operational, and public policy challenges. This approach aims to create an optimal ecosystem for innovation in AI in healthcare while respecting human rights, ensuring people's safety, and promoting equity in healthcare systems.

05. ACKNOWLEDGEMENTS

Thanks for contributing their knowledge to the development of this document to Félix Rígoli (FIOCRUZ), Fernando Aith (University of San Pablo), Mercedes de los Santos (Open Data Charter), Renato Berrino Malaccorto (Open Data Charter), Laura Alonso Alemany (National University of Córdoba), Daniel Otzoy (RECAINSA), Mauricio Farez (ENTELAI), Marcelo D'Agostino (OPS/PAHO), María Cristina Pombo (BID) y May Chomali (CENS).

06. BIBLIOGRAPHY

1. Alegsa L. Definición de Petabyte. Alegsa.com.ar. Published 18 de junio de 2023. Accedido noviembre 30, 2023. <https://www.alegsa.com.ar/Dic/petabyte.php>
2. Cabello S. Análisis de los modelos de gobernanza de datos en el sector público: Una mirada desde Bogotá, Buenos Aires, Ciudad de México y São Paulo. Documentos de Proyectos (LC/TS2023/71), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL). Published online 2023. <https://repositorio.cepal.org/server/api/core/bitstreams/9e5b987c-9168-4f88-9503-ca05c6d353ce/content>
3. Eastwood B. How to Navigate Structured and Unstructured Data as a Healthcare Organization. Publisher. Published 8 de mayo de 2023. Accedido noviembre 30, 2023. <https://healthtechmagazine.net/article/2023/05/structured-vs-unstructured-data-in-healthcare-perfcon>
4. García Zaballos A, Iglesias Rodriguez E, Puig Gabarró P. Informe anual del Índice de Desarrollo de la Banda Ancha: IDBA 2020: Brecha digital en América Latina y el Caribe. Inter-American Development Bank; 2021. doi:10.18235/0003337
5. Closing The Digital Gap (CTDG). Closing The Digital Gap (CTDG). Accedido noviembre 30, 2023. <https://closingthedigitalgap.org/>
6. United Nations. Sustainable Development Goals. un.org. Published 22 de agosto de 2018. Accedido noviembre 30, 2023. <https://www.un.org/sustainabledevelopment/es/sustainable-development-goals/>
7. Organización Panamericana de la Salud. Ocho principios rectores de la transformación digital del sector de la salud. Un llamado a la acción panamericana. Published online 2021. https://iris.paho.org/bitstream/handle/10665.2/53730/OPSEIHIS210004_spa.pdf?sequence=1&isAllowed=y
8. UNESCO. Ética de la inteligencia artificial. UNESCO. Published 13 de septiembre de 2023. Accedido noviembre 30, 2023. <https://www.unesco.org/es/artificial-intelligence/recommendation-ethics>
9. OECD. OECD AI Principles overview. OECD. Accedido noviembre 30, 2023. <https://oecd.ai/en/ai-principles>

10. World Health Organization. WHO outlines considerations for regulation of artificial intelligence for health. World Health Organization. Accedido noviembre 30, 2023. <https://www.who.int/news/item/19-10-2023-who-outlines-considerations-for-regulation-of-artificial-intelligence-for-health>
11. Filmus D, Schapachnik F. Inteligencia Artificial: el debate principal es cómo se regula y democratiza. Argentina.gob.ar. Published 2 de agosto de 2023. Accedido noviembre 30, 2023. <https://www.argentina.gob.ar/noticias/inteligencia-artificial-el-debate-principal-es-como-se-regula-y-democratiza>
12. PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO: relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Diario Oficial de la Unión Europea. <https://www.boe.es/doue/2016/119/L00001-00088.pdf>
13. RED IBEROAMERICANA DE PROTECCIÓN DE DATOS. ESTÁNDARES DE PROTECCIÓN DE DATOS PERSONALES PARA LOS ESTADOS IBEROAMERICANOS. Red Iberoamericana de Protección de Datos. Published online 20-JUNIO-2017. https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf
14. Transform Health. Principios de Gobernanza de Datos de Salud. Health Data Principles. Accedido noviembre 30, 2023. <https://healthdatapinciples.org/sp/about>
15. Mariano Díaz R, Núñez Reyes G. Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe. Published online 23 de agosto de 2023. Accedido noviembre 30, 2023. <https://hdl.handle.net/11362/49086>
16. Brodersen J. Tras el hackeo al PAMI, ciberdelincuentes publican información robada: hay historias clínicas, estudios y datos personales. clarin.com. Published 19 de agosto de 2023. Accedido noviembre 30, 2023. https://www.clarin.com/tecnologia/hackeo-pami-ciberdelincuentes-publican-informacion-robada-historias-clinicas-estudios-datos-personales_0_oVEAPipTS0.html
17. Ownby J. Hackeo masivo en Colombia: “La información de millones de personas está en manos de delincuentes en este momento”. El Pais. Published 14 de septiembre de 2023. Accedido noviembre 30, 2023. <https://elpais.com/america-colombia/2023-09-14/hackeo-masivo-en-colombia-la-informacion-de-millones-de-personas-esta-en-manos-de-delincuentes-en-este-momento.html>

18. Díaz RM. Estado de la ciberseguridad en la logística de América Latina y el Caribe. Accedido noviembre 30, 2023. <https://repositorio.cepal.org/server/api/core/bitstreams/4b04fcfe-c0f3-4c97-af14-2c234857f433/content>
19. Carnicero J, Serra P. Gobernanza de La Salud Digital: El Arte de La Transformación de Los Sistemas de Salud. Inter-American Development Bank; 2020. doi:10.18235/0002661
20. Broadband Commission. Reimagining Global Health through Artificial Intelligence: The Roadmap to AI Maturity.
21. Gómez Mont C, Del Pozo CM, Martínez Pinto C, Martín del Campo Alcocer AV. La inteligencia artificial al servicio del bien social en América Latina y el Caribe: Panorámica regional e instantáneas de doce países. Inter-American Development Bank; 2020. doi:10.18235/0002393
22. Administrative Department of the Presidency of the Republic (DAPRE). Artificial Intelligence Task Force. Presidency of the Republic of Colombia. Accedido noviembre 30, 2023. <https://inteligenciaartificial.gov.co/en/>
23. Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, Gobierno de Chile. POLÍTICA NACIONAL DE INTELIGENCIA ARTIFICIAL.
24. Cordeiro M. Brasil publica estrategia de Inteligencia Artificial. Accedido noviembre 30, 2023. <https://dplnews.com/brasil-publica-su-estrategia-de-inteligencia-artificial/>
25. Estrategia de Inteligencia Artificial. Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. Accedido diciembre 5, 2023. <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-inteligencia-artificial>
26. Quiénes somos. fairlac.iadb.org. Accedido noviembre 30, 2023. <https://fairlac.iadb.org/quienes-somos>
27. Tecnico D. Inteligencia Artificial (IA) Responsable: Claves para aplicar los principios éticos en las soluciones de IA en el campo de la salud. Accedido noviembre 30, 2023. https://clias.iecs.org.ar/wp-content/uploads/2023/11/DT3_CLIAS.pdf
28. Bagolle A, Park M, Marti M. Dashboard - Regulatory Frameworks for Digital Health in Latin American and the Caribbean: Electronic Health Records: Progresses and Next Steps. Dashboard - Social Digital. Accedido noviembre 30, 2023. <https://socialdigital.iadb.org/en/sph/dashboard>

07. ANNEX

Regulations on the Use of Health Data in Latin America and the Caribbean.

	Protection of Personal Data and Secondary Use of Health Information				Role of Patients in Relation to Their Health Data				Standards for EHRs and Interoperability	
	Personal data protection	National-Level Information Exchange	Security in the Storage of Health Data	Secondary Use of Health Information	Consent for the Use of Health Data	Patient Identification and Authentication	Patients' Rights to Edit Their Information	Patients' Access to Their Health Data	Interoperability and Standards	Codes and Standards for Health
Argentina	Ley 25326 de Protección de datos personales	Ley 26529 de Derechos del paciente Ley 25326 de Protección de datos personales	Ley 26529 de Derechos del paciente Ley 25326 de Protección de datos personales	Ley 25326 de Protección de datos personales	Ley 26529 de Derechos del paciente Ley 25326 de Protección de datos personales	Ley 26529 de Derechos del paciente	Ley 26529 de Derechos del paciente	Ley 26529 de Derechos del paciente	Resolución 680/2018 Resolución 115/2019	Resolución 680/2018
Bahamas	Acta de protección de datos (privacidad de la información personal)	Acta de protección de datos (privacidad de la información personal)	Acta de protección de datos (privacidad de la información personal)	Acta de protección de datos (privacidad de la información personal)	Acta de protección de datos (privacidad de la información personal)	Acta de protección de datos (privacidad de la información personal)	Acta de protección de datos (privacidad de la información personal)	Acta de protección de datos (privacidad de la información personal)	No data	No data
Barbados	Ley de Protección de Datos	Ley de Protección de Datos	Ley de Protección de Datos	Ley de Protección de Datos	Ley de Protección de Datos	Ley de Protección de Datos	Ley de Protección de Datos	Ley de Protección de Datos	No data	No data
Belize	Plan Estratégico del Sector Salud 2014-2024 Ley de Libertad de información	Plan Estratégico del Sector Salud 2014-2024	No data	No data	No data	No data	No data	No data	No data	No data
Bolivia	Decreto Supremo 1793 que reglamenta Ley 164	No data	Decreto Supremo 1793 que reglamenta Ley 164	Decreto Supremo 1793 que reglamenta Ley 164	Ley 164 para el Desarrollo de Tecnologías de Información y Comunicación	No data	Ley 164 para el Desarrollo de Tecnologías de Información y Comunicación	Ley 164 para el Desarrollo de Tecnologías de Información y Comunicación	No data	No data
Brazil	Ley 13709	Directiva 2073 Ley 13709	Ley 13709 Ley 13787	Ley 13709	Ley 13709	Ley 13709	Ley 13709	Ley 13709	Directiva 2073	Directiva 2073
Chile	Ley 19628 Decreto con Fuerza de Ley 1	Ley 19628 Decreto con Fuerza de Ley 1	Ley 19799 Decreto Supremo 83 Decreto 41	Ley 19628	Ley 20584 Ley 19628	Decreto 41 Decreto 643	Ley 19628	Decreto 41	Decreto 643	Decreto 643
Colombia	Ley 1581 Ley 2015 Res. 839/17 Decreto 1377/13	Ley 2015	Ley 1995 Ley 1413 Ley 1581 Ley 2015	Ley 1581	Ley 1581 Decreto 1377/13	Regulación N°12 de 2013 del Ministerio de Salud	Ley 1581 Decreto 1377/1	Ley 1581 Decreto 1377/1	Ley 2015	Sin datos
Costa Rica	Ley 9162 Regulaciones de la Historia Clínica Digital Unificada	Ley 9162	Ley 9162 Regulaciones de la Historia Clínica Digital Unificada Ley 8968	Ley 8968	Sesión 7366-1999 Ley 8968	Ley 9162	Ley 8968	Ley 8968 Ley 8239	Regulación 39652-S-MICIT	Regulación 39652-S-MICIT
Dominican Republic	Ley 172-13	Ley 172-13	Ley 172-13	Ley 172-13	Ley 172-13	Ley 172-13	Ley 172-13	Ley 172-13	No data	No data
Ecuador	Regulación 00005216-A	Regulación 00005216-A	Regulación 00005216-A	Regulación 00005216-A	Constitución Nacional	Regulación 0009-2017	No data	Regulación 0009-2017	Regulación 0009-2017	Regulación 0009-2017

CHALLENGES AND RECOMMENDATIONS IN DATA GOVERNANCE FOR THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE IN HEALTH IN LATIN AMERICA AND THE CARIBBEAN

					Regulación 0005216-A				Regulación 00001190	Regulación 00001190
El Salvador	Resolución 941 Decreto307	Resolución 941	Resolución 941 Decreto 133	Decreto 307	Resolución 941	Resolución 941	Resolución 941	Resolución 941	No data	No data
Guatemala	Decreto 57-2008	No data	No data	Decreto 57-2008	Decreto 57-2008	No data	Decreto 57-2008	Decreto 57-2008	No data	No data
Guyana	Acta 21 de acceso a la información	Acta 21 de acceso a la información	No data	No data	Acta 21 de acceso a la información	No data	Acta 21 de acceso a la información	Acta 21 de acceso a la información	No data	No data
Haití	No data	No data	No data	No data	No data	No data	No data	No data	No data	No data
Honduras	Decreto170-2006	No data	No data	Regulación 65-91	Decreto 170-2006	No data	Decreto 170-2006	Decreto 170-2006	No data	No data
Jamaica	Acta 2020 de protección de datos	Acta 2020 de protección de datos	Acta 2020 de protección de datos	Acta 2020 de protección de datos	Acta 2020 de protección de datos	Acta 2020 de protección de datos	Acta 2020 de protección de datos	Acta 2020 de protección de datos Acta de acceso a la información	No data	No data
Mexico	Ley DOF 05-07-2010	NOM-024-SSA3-2010	NOM-024-SSA3-2010	NOM-024-SSA3-2010	DOF 11-01-2012	NOM-024-SSA3-2010	DOF 11-01-2012	DOF 11-01-2012	NOM-024-SSA3-2010	NOM-024-SSA3-2010 NOM-024-SSA3-2012
Nicaragua	Regulaciones de la Ley 787 Ley 423	Regulaciones de la Ley 787	Regulaciones de la Ley 787	Regulaciones de la Ley 787	Regulaciones de la Ley 787	No data	Regulaciones de la Ley 787	Regulaciones de la Ley 787	No data	No data
Paraguay	Ley 1682	No data	No data	Ley 1682	Ley 1682	No data	No data	Ley 1682	No data	No data
Peru	Ley 29733	Ley 30024 Decreto Supremo 009-2017-SA	Ley 30024 Decreto Supremo 009-2017-SA	Ley 30024 Decreto Supremo 009-2017-SA	Ley 29414 Ley 26842	Decreto Supremo 024-2005-SA Decreto Supremo 009-2017-SA	Ley 30024 Ley 29414 Ley 26842	Ley 30024 Decreto Supremo 009-2017-SA	Ley 30024 Decreto Supremo 009-2017-SA	Resolución ministerial 469-2019/MINSA
Suriname	No data	No data	No data	No data	No data	No data	No data	No data	No data	No data
Uruguay	Ley 1831 Decreto 242/017	Ley 19355 Decreto 242/017	Decreto 242/017	Decreto 242/017	Ley 18335 Ley 18331	Decreto 242/017	Decreto 242/017Ley 18331	Decreto 242/017	Decreto 242/017	Decreto 242/017
Venezuela	Acta de Telesalud Decreto 9051	Acta de Telesalud Decreto 9051	Acta de Telesalud	Decreto 9051	Decreto 9051	No data	Decreto 9051	No data	Acta de Telesalud Decreto 9051	Sin datos
Regional average! LAC (%)	88.46%	72.92%	73.07%	84.61%	88.46%	61.53%	73.07%	84.61%	42.3%	30.76%

Source: Own elaboration based on IDB Map²⁸