GOVERNANCE

IDB

REGULATORY FRAMEWORKS

FOR DIGITAL HEALTH IN LATIN AMERICAN AND THE CARIBBEAN

Electronic health records:
progresses and next steps

Authors: Alexandre Bagolle, Mihwa Park and Myrna Marti.
Design: www.souvenirme.com

GOVERNANCE

IDB

REGULATORY FRAMEWORKS

FOR DIGITAL HEALTH IN LATIN AMERICAN AND THE CARIBBEAN

Electronic health records:
progresses and next steps

Contents

Introduction

One of the most promising aspects of digital health is the possibility of creating comprehensive, high-quality, and patient-centered health systems. To make this possibility a reality and thus enhance the quality and efficiency of health systems, fluid and secure data management is crucial. To progress toward efficient and patient-centered digital health models, the right stakeholders need access to the right information at the right time. This timely access to high-quality data is essential if the system's stakeholders are to make better decisions and provide higher quality services (Nelson *et al.*, 2020).

A key component of digital health systems is electronic health record (EHR) systems.[1] EHR are digital systems specifically designed to record, store, and analyze data, assessments, and information about events related to people's health and diseases and the actions resulting from these events. They are thus much more than a digital version of paper health records because they enable accessibility, provide support for multiple appointments, improve communication between providers and patients, allow data to be consolidated, provide access to knowledge bases, and can be integrated into decision-support tools (Nelson *et al.*, 2020; ISO, 2014).

EHR systems are an essential primary source of health data, providing information on people's journey through the system and ensuring continuity of care for patients. They are also a key to empowering patients because they allow them to access to their medical information, record or track their symptoms, and manage their own appointments (Chá Ghiglia, 2019).

Well-designed and well-executed systems can break down the many data silos that create inefficiencies throughout the entire health system. Complete and interoperable electronic health records let users access and exchange data in the whole public health system, giving them a rapid and accurate picture of the public health events in a given population. With EHR health information is accessible and available in real time; is legible and can be displayed in multiple ways; and is secure and can be integrated with other components of the information system, all of which makes more comprehensive prevention, containment, and mitigation actions possible. EHR systems are also key to supporting other digital health initiatives, like telehealth, because the EHR systems give different providers the access to patient information they need and provide crucial data for improving the quality of processes and services. They can also provide information for improving health system management, surveillance, and public health research (PAHO, 2014; Nelson *et al.*, 2020).

[1] Other terms used for EHR include: electronic medical record, electronic medical history, digital medical record, electronic medical file, and digital health file.

Given the potential benefits of EHR systems, it is critical that countries in Latin America and the Caribbean (LAC) have strong regulatory frameworks that enable and facilitate the implementation and use of EHR systems at all levels of the health system.

However, developing clear and effective regulatory frameworks for digital health is a highly complex undertaking for at least three reasons:

- **Novelty:** The data revolution and the challenges related to big data, the wide range of formats and content, and the speed at which data is produced is a relatively recent reality (Silcox, 2020). Developing regulatory frameworks for digital health is therefore a work in progress and an ongoing learning experience based on trial and error, since there are still few experiences and lessons to learn from.

- **Variety:** Digital health is a multifaceted reality covering aspects ranging from clinical considerations to information technology and other technologies, as well as organization, managing data or rights, and the obligations of patients and health professionals (Carnicero & Serra, 2020).

- **Balance between the flow and protection of data:** When developing regulations, countries find they need to strike a certain balance between different objectives that may seem to be at cross purposes. For example, health data is especially sensitive personal data and *must* be protected, but at the same time, it also has to be able to flow easily to improve the quality and continuity of care. The major challenge for countries is finding a legal formula that is well suited to the context and characteristics of the health system in each country and that allows people's health data to move fluidly in a protected and secure environment.

The specialized literature has focused on regulatory aspects related to digital health, identifying in advance potential legal and technical risks to privacy and security linked to digitalizing personal medical information (Appari *et al*., 2010) and using EHR (Hiller *et al*., 2011). Since it contains sensitive personal health information, EHR data must be protected by regulations covering accessibility, security, privacy, and replicability, among other aspects (Hoffman *et al*., 2012; Hoffman *et al*., 2008; Terry *et al*., 2006). Different studies attempt to systematically review the legal frameworks for EHR in different regions of the world, including Europe (EU, 2014) and Latin America and the Caribbean (RACSEL, 2018; Borbolla *et al*., 2019).

The European Union (EU) study provides systematized information on the legal framework of 28 countries (EU, 2014). According to this study, there are major disparities in the EU countries' legal approaches to regulating EHR. While some countries have specific laws governing EHR, others regulate the matter under general data protection laws. The study analyzes European countries' progress on accessing, storing, and exchanging health information, as well as its security. While the evidence needs updating in light of for example, recent changes in the field of data protection, with the adoption of the General Data Protection Regulation, or other developments related to exchanging health data- the study provides important parameters for systematically analyzing regulatory aspects related to digital health in other regions.

Similar efforts to analyze the legal frameworks for digital health and EHR have been launched in Latin America and the Caribbean. The Digital Health Cooperation Network of the Americas (Red Americana de Cooperación sobre Salud Electrónica-RACSEL) proposes a series of key dimensions for a legal framework fostering the implementation of EHR and proposes an analysis of the current laws in 5 countries in the region (RACSEL, 2018). Borbolla *et al*. (2019) analyzes the legal framework of 21 countries in the region and identifies the progress made on data protection and other aspects that need to be developed to enhance the exchange of and access to patients' health data. These studies are major steps forward for analyzing the legal framework for EHR in countries in the region, and they complement each other. Although they differ on a few specific aspects, the two studies analyze similar dimensions of the legal frameworks of Latin American countries and lay the groundwork for defining the key elements

of a model regulatory framework for the region. Methodologically speaking, RACSEL is based on an analysis of the different countries' legal texts, while Borbolla *et al*. is based on secondary data from surveys and interviews with health information system experts, providing two complementary views on the topic. Borbolla *et al*. covers a large number of countries but does not closely examine the texts of the actual laws. Meanwhile, RACSEL covers fewer countries but analyzes the legal content of the national regulatory frameworks in greater depth.

This document aims to explore these findings in greater depth and contribute to the analysis of the progress made and work still to be done on the regulations of countries in Latin America and the Caribbean. This study maps out the existing regulations in the countries in the region, identifies different strengths and opportunities for improvement, and gives a set of recommendations and suggests the next steps. The ultimate goal of this study is to foster an exchange of best practices and lessons learned in the region. The countries in the region will only be able to respond to the challenges of digital health and take advantage of immense possibilities of digital health by engaging in this collective and ongoing learning process. While this first study focuses on EHR and all regulations that touch on its operation, it lays the foundation for more extensive future studies that cover topics like telehealth, artificial intelligence, and cyber security, among others.

This study is complemented by an interactive online tool that allows readers to navigate between the different laws and texts that make up the regulatory framework of countries in the region and analyze the statistics presented in this document in greater detail.

To access the online tool, click on the image below. The tool is also referenced in several other sections of the document.

The first section of the document lays out a conceptual reference framework based on the findings of the literature on this topic and presents the methodology used for the study (Section I). Then this conceptual framework is used to propose an analysis of progress made on developing regulatory frameworks in the region, as well as the challenges in this area (Section II). Section III provides more detailed analysis of how different countries in the region handled key legal aspects of EHR in their regulatory frameworks. Finally, the last section contains conclusions and a set of recommendations (Section IV).

Section 1: The study's conceptual reference framework and methodology

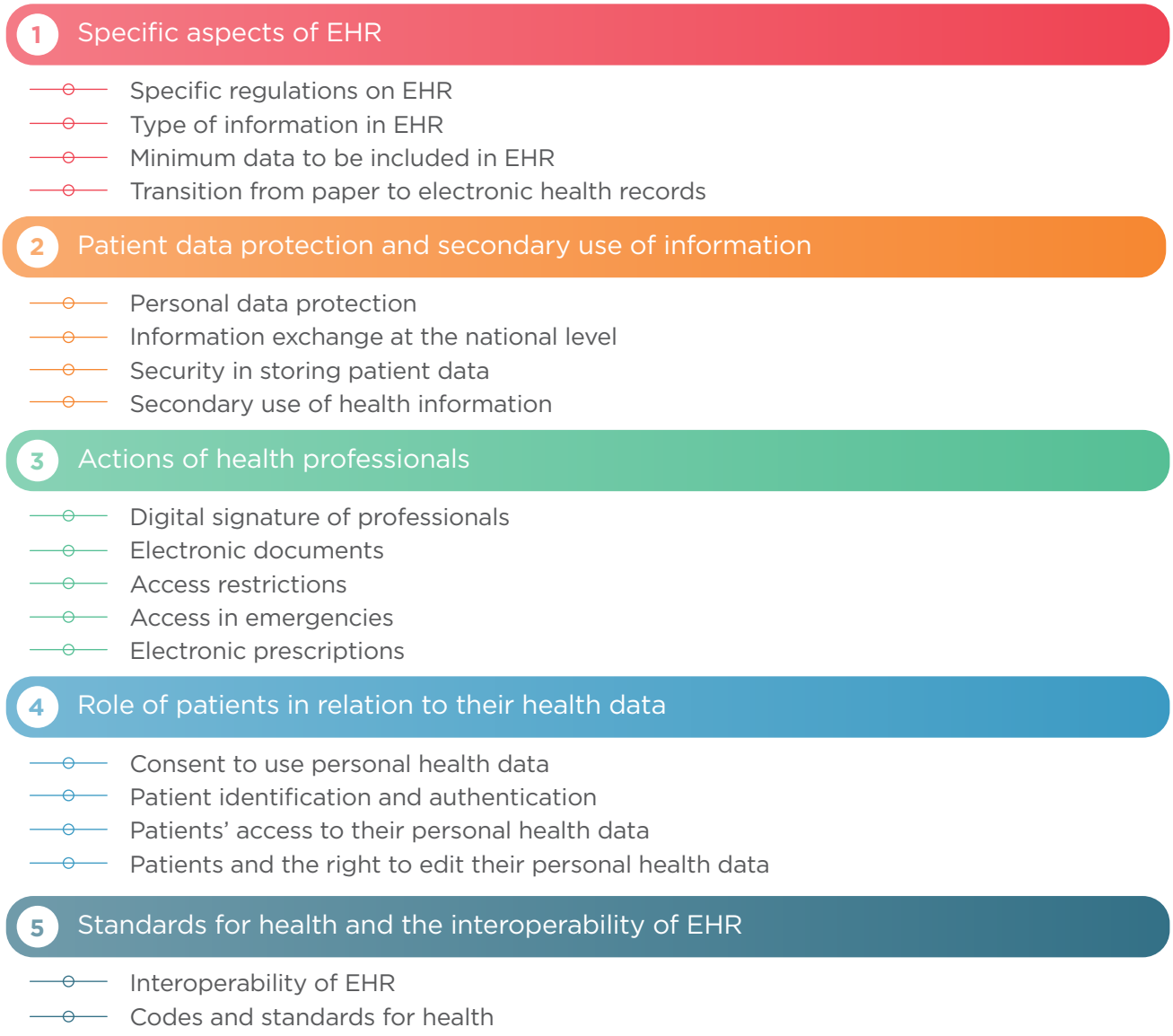
>> a) Conceptual framework

In recent years, different conceptual frameworks have been proposed for analyzing regulations on digital health in general and on the implementation of EHR systems in particular. The aim of these conceptual frameworks is to identify key aspects to be addressed in a country's legal system to enable the correct implementation of an EHR system. A review of existing conceptual frameworks reveals a general consensus in the literature about the fundamental dimensions that should be included in regulations on EHR.

The study by Borbolla *et al*. (2019) proposes a conceptual framework organized around 5 dimensions: specific legislation on electronic medical records, patient data protection and secondary uses of information, legislation on the actions of healthcare professionals, legislation on the role of patients, and, lastly, regulations on the use of standards in the area of health and programs for promoting electronic medical records. Each dimension can be broken down into 16 sub-dimensions. The Digital Health Cooperation Network of the Americas (RACSEL, 2018) proposed a set of 11 key dimensions that match and complement the dimensions proposed by Borbolla *et al*. The dimensions proposed by RACSEL include establishing the rights of patients whose information is contained in EHR, personal data protection, information exchange, keeping information safe and secure, use of electronic documents and signatures, and use of standards, among others. Other prior studies, such as those by the WHO (2016) or the European Union Health Programme (EU, 2014) had already identified similar dimensions, including those related to the content and interoperability of EHR, security, patient consent or access, and using and exchanging health information.

In light of the existing frameworks, **Figure 1** proposes an integrated conceptual reference framework with five main categories divided into 19 dimensions. Based on the findings of the existing studies, this conceptual reference framework attempts to propose an integrated version of the essential dimensions that a regulatory framework for implementing EHR should contain, according to the specialized literature. Each of the proposed dimensions has been highlighted in some or all of the existing studies on the topic (Borbolla *et al*., 2019; RACSEL, 2019; HPEU, 2014; WHO, 2016).

FIGURE 1 • Conceptual reference framework: 5 categories and 19 dimensions.



These 5 categories and their respective dimensions capture the complexity and diversity of the topics that regulatory frameworks need to address in order to implement EHR:

Specific aspects of EHR: This category covers specific legislation on EHR that generally brings together and systematizes all provisions on implementing EHR at the national level in a single legal text. These provisions include, at minimum, a definition of what a nationwide EHR is, its characteristics, the type of information and data it contains, and ideally, a mandatory minimum basic data set (MBDS) for EHR.[2] This category also encompasses provisions on the transition from paper to electronic records and the role of the different stakeholders involved in implementing it.

Patient data protection and secondary use of information: This category includes the regulations governing the protection of people's data, of which health data is recognized as an especially sensitive subset. It also includes provisions on guaranteeing the privacy and confidentiality of that data, as well as those governing its secure storage and transfer. Regulations governing secondary uses of people's data include those

[2] Though there is no one single formula, generally the MBDS includes: the usual demographic data (age, sex, place of residence), as well as data on diagnosis, risk factors, procedures, the patient's date of admission and discharge, and type of admission and discharge (RACSEL, 2019)

covering the processing of that information for scientific research, statistics, public health, epidemiology, public opinion surveys and polls, or market studies, among other uses. The regulations in this category include *habeas data* laws or data protection laws that, though not specifically about health, have a broad scope of application and are an umbrella under which all regulations on data are developed.

Actions of health professionals: This category includes regulations recognizing the legal validity of electronic signatures and documents as evidence, and provisions governing their legal effects. It encompasses provisions on electronic identification and authentication and on defining professionals' roles and levels of permissions and access. This category also includes regulations on implementing and using electronic prescription systems.

Role of patients in relation to their health data: This category includes legal provisions on the requirement of consent in order to process people's health data. The issues of identifying and authenticating patients, rights to access, and the editing, rectification, and erasure of personal health data by data subjects also fall under this category. As in other categories, the regulations in this category include data protection laws or information access laws that are not specific to health but contain provisions and articles related to health data.

Standards for health and interoperability of EHR: This category encompasses matters related to technical, semantic, syntactic, and organizational interoperability, and the role of stakeholders in charge of encouraging the adoption of standards, codes, and terminology. It includes legal provisions on the inter-operable nature of the EHR system, and articles and other technical documents with legal validity that address the type of standards to be used to effectively make the EHR inter-operable.

>> b) Methodology and interpretation of data

Based on this conceptual framework, the authors analyzed the existing regulations in 26 Latin American and Caribbean countries, most of which are available on each country's official legal information web portal.[3] All enacted legislation was included in the search, regardless of when it went into effect. The authors first researched each country's regulations in each of the five categories of the conceptual framework. They looked for regulations in each country related to EHR specifically, on patients' data protection and secondary use of information, on the actions of health professionals, on the role of patients in relation to their EHR, and regulations on standards for health and the interoperability of EHR. This initial search yielded a database of 115 regulatory texts, which were primarily laws, decrees, resolutions, and directives. This database is the primary source of information for this study.

The second step was to analyze the legislation that had been compiled by applying the conceptual reference framework laid out in **Figure 1**. For each country, the authors identified which of the 19 dimensions are covered by existing regulations and pinpointed the specific legal texts and articles that address those dimensions. This made it possible to compare each country's regulations with the conceptual reference framework to shed light on the progress made at a regional level, as well as on possible regulatory gaps and areas for improvement in the future.

Finally, based on this legal analysis, the authors created indicators to make it easier to interpret the progress made by countries in the region and their future challenges. The indicators have two complementary approaches. The first is a regional approach that gives a combined overview of the regulations in all 26 countries

[3] The study covers the following countries: Argentina, Bahamas, Barbados, Belize, Bolivia, Brazil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Guyana, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Dominican Republic, Suriname, Trinidad and Tobago, Uruguay, and Venezuela. Some countries in the region have legal information portals that centralize laws, decrees, and other national regulations. In these cases, the portals were used as an official primary source. In countries where this type of portal does not exist, searches were done using other channels, like health ministry websites, official gazettes or their equivalent, and national media. The database of regulations used in this study is up-to-date as of March 2020.

analyzed. This first approach reveals regional challenges in relation to digital health legislation and highlights a set of crosscutting lessons. The second approach focuses on the national level and shows the number of dimensions in the conceptual framework that are covered in a given country's regulatory framework. The second approach gives an overview of the progress and shortcomings of national regulations and makes it possible to identify specific lessons and recommendations for a given national context. The combination of both approaches enables recognition of opportunities for exchanging experiences and lessons learned between countries in the region.

Before analyzing and interpreting the results of the analysis in more detail, it is important to bear in mind the scope and limits of this methodology. The methodology used makes it possible to map out and summarize the progress made by countries in the region, as well as to analyze whether a key dimension of the conceptual reference framework is present in a country's legal framework. In this sense, it is a descriptive and cartographic analysis of the regulations. What it does not provide are conclusions on whether that dimension is *properly* addressed and covered by the regulatory framework in question. The methodology describes what is, but it does not analyze in detail the *quality or maturity level* of each dimension within the different national regulatory frameworks included in the study. This study is an initial mapping of the regulatory landscape that aims to lay the foundation for future and more detailed analyses of the maturity of each country's regulatory framework. Lastly, this analysis does not aim to rank countries, but rather to identify progress and challenges shared by all countries in the region to foster collective learning and an exchange of information and lessons learned between countries, facing the new and complex challenges of the era of digital health.

Section 2: A regional perspective on regulatory progress

The regional analysis yields a series of overarching lessons about progress on EHR regulations.

While a large majority of LAC countries have made progress on one or more of the key dimensions in the conceptual framework, they are moving forward at different paces. Some included all or nearly all the dimensions in the conceptual framework in their regulations, while others cover a more limited number. Countries can thus be roughly classified into groups to sum up the region's regulatory successes and challenges. The analysis also found that certain dimensions are more developed than others, that much more progress has been made in some categories and dimensions of the regulatory framework than in others.

>> a) Uneven progress between countries in the region

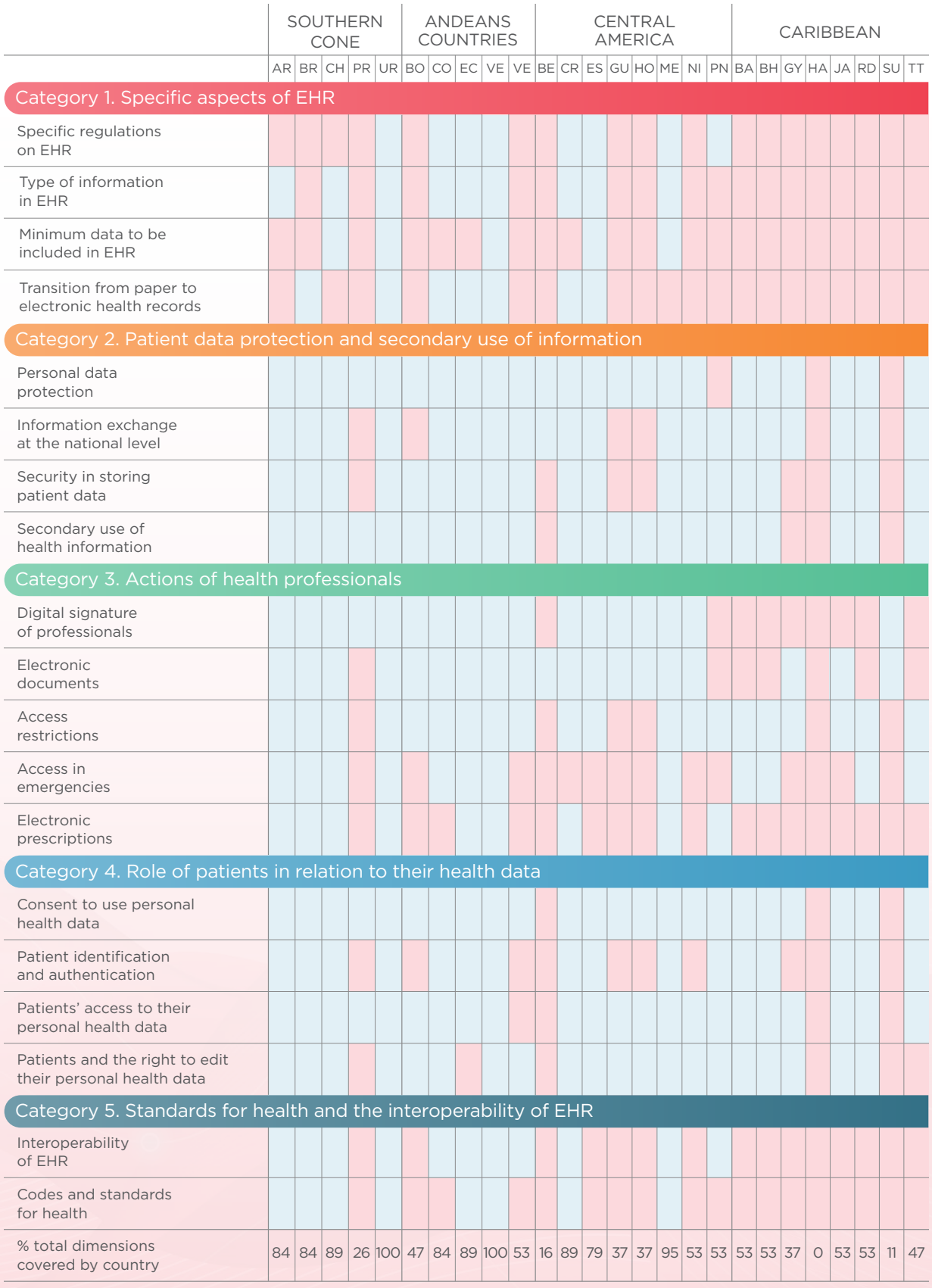
Of the countries analyzed, 10 out of 26 countries enjoyed advanced regulatory frameworks that cover more than 75% of the key dimensions of the conceptual reference framework. Argentina, Brazil, Chile, Colombia, Costa Rica, Ecuador, Mexico, Peru, El Salvador, and Uruguay fall into this first group of countries with highly developed regulatory frameworks that address a large majority of these dimensions. Most of these countries have had specific, national regulations governing the implementation and use of EHR for several years. In many cases, these regulations are comprehensive and cover most of the important dimensions in detail or reference other regulations; such as using and exchanging health data, on patient rights, and on the actions of healthcare professionals. Mexico, for example, approved Official Mexican Standard NOM-024-SSA3-2010 in 2010. It "establishes the functional objectives and functionalities that products of the Electronic Health Record Systems should have in order to guarantee the interoperability, processing, interpretation, confidentiality, and security of information in electronic health records, as well as the use of standards and catalogs for that information." Costa Rica passed Law No. 9162 on "Unified Digital Health Records" in 2013. The same year, Peru passed Law No. 30024, which "creates the national registry of Electronic Health Records," and its regulations were set forth in Supreme Decree No. 009-2017-SA of 2017. Also in 2017, Uruguay passed Decree No. 242/017, the purpose of which is to "regulate aspects related to the electronic processing and exchange of personal information by public and private institutions with legal authority over health-related matters, as well as the National Electronic Health Records System and its Platform." Unlike the other countries in this group, Argentina, Brazil, and Chile do not have a specific primary regulation on EHR. Instead, the main legal dimensions are governed by a set of complementary and interrelated laws.

In the second group, 7 countries in the region have advanced regulatory frameworks that address between 50 and 75% of the dimensions in the conceptual reference framework. These countries do not have a specific regulation on EHR, but they have made important progress on other dimensions of the conceptual reference framework, especially patient data protection and secondary use of information, patients' role in relation to their health data, and, to a lesser

extent, the actions of health professionals. This group of countries, consisting of the Bahamas, Barbados, Jamaica, Nicaragua, Panama, the Dominican Republic, and Venezuela, have, however, significant room to improve on aspects specific to EHR and on interoperability and the use of standards.

FIGURE 2 • Regional map of the progress made in regulatory matters.

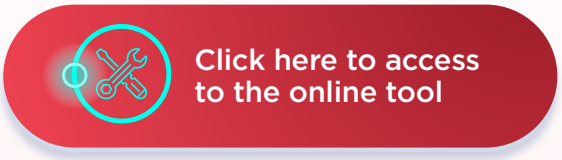
FIGURE 3 • An overview of the regulatory frameworks of the 26 countries in the region.



In the third group, 6 countries in the region have regulatory frameworks that address between 25% and 50% of the dimensions in the conceptual framework. This group is composed of Bolivia, Guatemala, Guyana, Honduras, Paraguay, and Trinidad and Tobago. Like the second group, its main regulatory strengths are data protection and patients' role in relation to their health data. However, these domains are less developed in this group of countries, and important aspects related, for example, to patient identification or securely storing patient data are missing from their regulations. They also lack regulations on aspects specific to EHR, on interoperability, and on the use of standards.

Lastly, there is a fourth group of 3 countries[4] (Belize, Haiti, and Suriname) with regulatory frameworks that cover less than 25% of the key dimensions in the conceptual framework. While these regulatory frameworks are at their very beginning stages, the countries in this group are not starting from scratch and they have made some progress on protecting patients' data and on regulations for digital signatures and/or electronic documents.

Figures 2 and 3 summarize the progress of the 26 countries in the 5 categories of the conceptual reference framework. Progress made and future challenges can be analyzed in depth using the interactive tool.



[4] Regarding the estimates for Haiti and Suriname, it is important to mention language-related difficulties, as well as the difficulties of accessing regulations via official portals.

>> b) Uneven progress between dimensions of the regulatory framework

Regional-level progress can also be analyzed based on the different dimensions of the conceptual framework. This perspective shows the areas where the region has accumulated the most experience and the dimensions with the most work yet to be done.

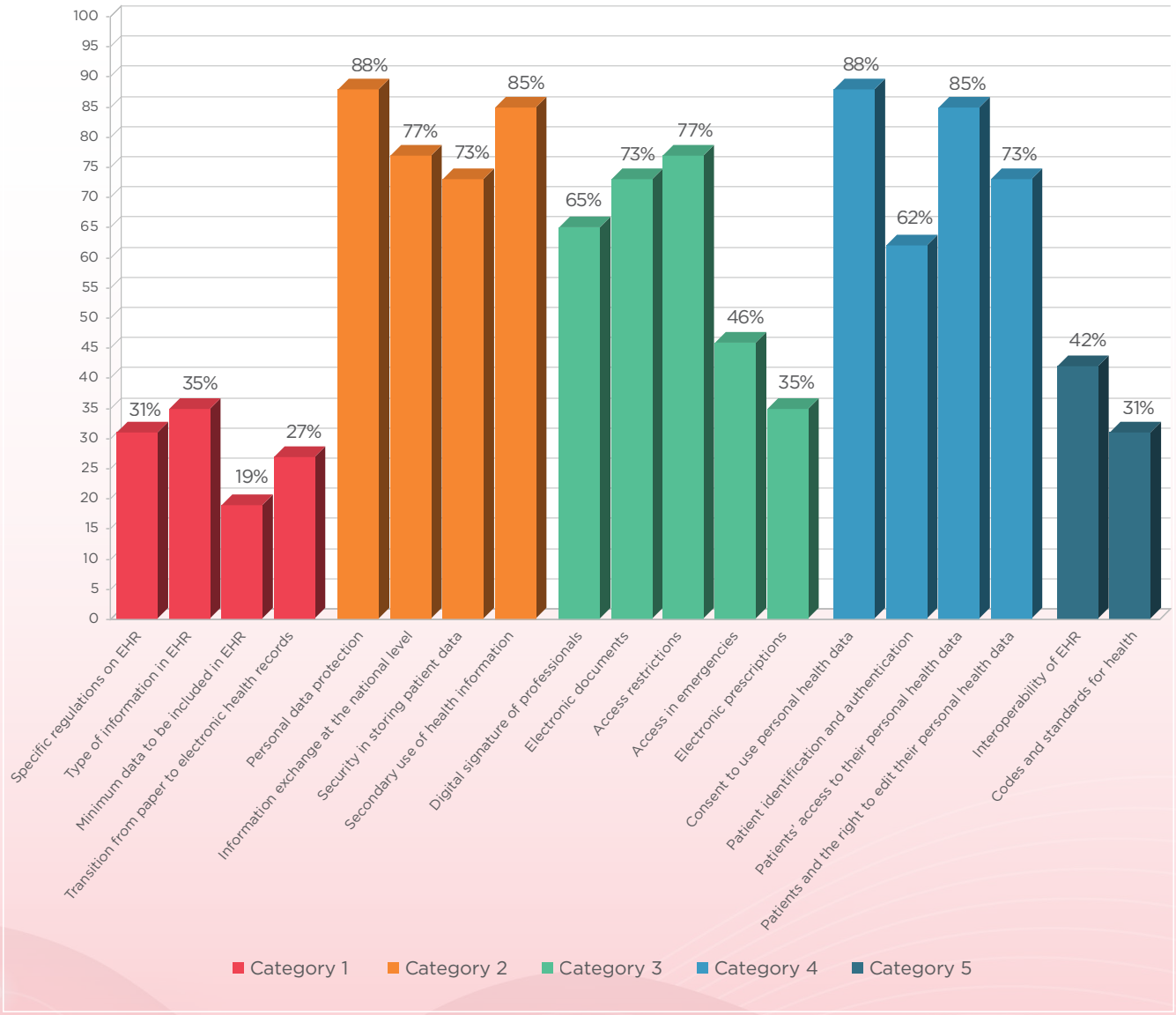
Figure 4 shows the percentage of countries in the region that address a given dimension in their national regulatory framework. The categories that are best represented in national regulatory frameworks are patient data protection and secondary use of information (category 2), actions of healthcare professionals (category 3), and the role of patients in relation to their EHR (category 4). Category 1 (specific aspects of EHR) and category 5 (Standards for health and interoperability of EHR) are the least addressed and developed among the different regulatory frameworks covered by this study.

It is noteworthy that 88% of the regulatory frameworks analyzed address the issue of protecting personal health data by, for example, recognizing the especially sensitive nature of health data, and 77% of countries have regulations on exchanging personal health data. Likewise, topics related to electronic documents, digital signatures, and controlling the access of healthcare professionals to health data (category 3) are also covered in detail by regulations. 73% of countries have regulations on electronic documents, and 65% have regulations on digital signatures. In category 4—on the role of patients—, 80% of the regulatory frameworks analyzed address patient rights and consent regarding the use of their health data.

Conversely, the most underrepresented dimensions in the regulatory frameworks in this study are related to the content of EHR. 31% of countries in the region have specific regulations on using EHR. Only 19% of the countries have begun establishing a minimum dataset to be exchanged in EHR, and 27% have any sort of regulations to address problems related to transitioning from paper medical records to EHR (category 1). Less than half of the countries covered the interoperability of EHR in their national regulatory framework, and 31% refer to using codes and standards (category 5). There is also significant room to improve in the areas of establishing regulations for electronic prescriptions (category 3) and patient identification (category 4).

This first section concludes with a series of region-wide lesson: First, it can be seen that 38% of the countries in the region have highly -developed regulatory frameworks that cover most of the key dimensions in the conceptual reference framework. Second, the countries that have made less progress chose to prioritize the development of aspects related to protecting patients' data and the role of patients in relation to their health data, and to a lesser extent, the actions of health professionals. Third, and as a result of the second conclusion, the least developed dimensions are those related to regulations specific to EHR, the content of EHR, the specific data to be exchanged, and the transition to digital formats, as well as the dimensions related to interoperability and using standards. These preliminary findings give an idea of LAC countries' regulatory progress and pending tasks.

FIGURE 4 • Regional progresses in the different dimensions of the conceptual framework of reference



Section 3: The countries and their approach to the dimensions of the regulatory framework

This section analyzes how the countries in the region address the different dimensions of the conceptual reference framework in their respective national regulations, finding similarities and differences between countries and taking a closer look at the wide variety of formulas the countries in the region have designed to tackle the new challenges of digital health.

Each subsection corresponds to the analysis of a category of the conceptual framework of reference. The relevant regulations of each country are available in the online tool.

>> a) Category 1. Specific aspects of EHR

As with any digital transformation process, implementing an EHR system involves a series of specific transformations related to processes, information management, governance, change management, roles of public and private stakeholders, infrastructure, and technological systems, all of which needs to be addressed in a regulatory framework. It is important not to confuse the process of implementing an EHR system with the process of digitalizing health records that were originally on paper. This section draws a distinction between two general groups of countries. The study first analyzes countries with specific regulations for implementing EHR, with their similarities and differences. It then examines countries that do not have specific regulations on EHR but that do regulate certain aspects relevant to implementing EHR (such as, for example, the validity of health records in digital format or the information to be included in EHR) in other legal texts that are part of their regulatory frameworks.

Countries with specific regulations on EHR. Certain countries like Colombia, Costa Rica, Ecuador, El Salvador, Mexico, Peru, and Uruguay developed specific regulations to facilitate the implementation of EHR systems. These regulations usually address a set of key topics like the legal definition of EHR and EHR's scope of application; the role of public actors in implementing the EHR system; the deadline for implementation and funding-related matters; the content, security, and confidentiality of EHR; identification and access; and interoperability and the use of standards. In other words, these regulations cover and systematize most, if not all, of the key dimensions identified in the conceptual framework in a single legal text. **Figure 5** summarizes the objective of these regulations, the nationwide definition of EHR they propose, and the main content and topics they cover. These specific regulations on implementing EHR systems are usually harmonically incorporated into a broader legal framework and reference other laws such as those on *habeas data*, the rights and obligations of patients and professionals, or others, which are analyzed in more detail in the following sections.

Of note is the wide variety of terms and definitions for EHR among the different countries in the region that developed a specific EHR regulation. For example, in article 2 of Decree No. 242/017, Uruguay defines EHR as "*the comprehensive set of medical, social, and economic*

data on a person's health, from their birth until their death, processed using electronic means, being the functional equivalent of the paper medical file." In NOM-024-SSA3-2010, Mexico defines "Electronic Health File" as "*the electronic means by which health personnel must register, log, and certify the action they took in relation to the patient, in accordance with the health regulations. It enables unified management of a single, longitudinal health record for each patient in digital format.*" Generally speaking, some definitions place more emphasis on the technological aspects of EHR, while others focus more on its informational content. What is clear is that there is no standardized nor unified concept of EHR among LAC countries.

Another aspect that varies between national regulations is their degree of precision and details regarding the information to be included in EHR. Certain countries like Colombia or Ecuador give general descriptions of content, such as, in the case of Ecuador, the "*detailed and orderly exposition of all data related to a patient or user; this includes information on the individual and their relatives, on their history, current status and changing condition, as well as the procedures and treatments they have undergone*" (Regulation 00005216-A, article 38). In contrast, countries like Mexico, Peru, or Uruguay specified the basic minimum health datasets to be included in EHR in greater detail. Article 8 of Uruguayan Decree 122/019 states that "*to generate electronic health documents, health institutions must include the minimum dataset specified in Appendix 1*," which defines the minimum dataset as the "*set of basic data that an electronic health document must contain, at minimum, in order to facilitate the continuity of care for users of the national integrated health system*," and it provides details on the information to be exchanged.

A common aspect of all the different national regulations analyzed is few details and specifications about how the transition between paper health records and EHR will be organized and implemented. Certain countries, like Costa Rica, specify the legal timeframes for implementation. The sole transition provision of Law No. 9162 on the Unified Digital Health Record establishes, for example, that "*the Costa Rican Social Security System shall have five years from when this law takes effect to ensure nationwide compliance with the objectives established in this law. The deadline for implementation at the primary care level is the first three years of this five-year period, and the unified digital health record must be implemented at the hospital level by the end of five years.*" Other countries, like Ecuador (see the sole general provision and transition provisions of Regulation No. 0009-2017) or Peru (see the supplemental provisions of Law 30024) establish that the paper format will continue to be used until the digital version of the health records, the IT systems, and the establishments' connectivity are ready. A large majority of countries do not address the transition at all in their regulations, and the authors found no legally valid information on the plans, roles, and responsibilities needed to ensure a successful transition from paper to digital systems. In other words, aspects related to change management (Baum & Giussi, 2019) were missing from the national regulatory frameworks.

Countries with no specific regulations on EHR but that recognize the validity of health records in digital format. Lastly, it is worth noting that while countries like Argentina, Brazil, and Chile have a regulatory framework that covers most of the key dimensions of the conceptual framework as a whole, they do not have a specific regulation on EHR. Argentina mentions the electronic format of health records in Law 26529 on "Patient Rights, Health Records, and Informed Consent" and proposes a set of key definitions in Resolution 189/2018 on "The National Digital Health Strategy 2018-2024" and Resolution 115/2019 on the "National Network for Interoperability in Health." In Brazil, Law 13787 authorizes the digitization of health records. In Chile, Law 20584, which "governs people's rights and duties in relation to actions linked to their healthcare" and Decree 41, which "approves the regulations on medical files" mention the possibility of keeping people's medical files in electronic format. While these regulations recognize the validity of the electronic format, they do not take into account set of key aspects that are specific to EHR such as, for example, how EHR is implemented, the role of public actors, or the content of EHR, as well as the issues of security, identification, and access, or of interoperability and the use of standards.

FIGURE 5 • A breakdown of the main regulations on specific aspects of EHR: objective, definitions, and main topics addressed

Colombia

Regulation	**Law 2015** — This law creates interoperable electronic health records and establishes other provisions.
Objective of the regulation	**Article 1.** The purpose of this law is to govern the Interoperability of Electronic Health Records (IHCE), which will be used to exchange relevant medical data, as well as the documents and clinical files generated over the course of each person's life.
Definition of EHR	An Electronic Health Record is a comprehensive and chronological record of a patient's health, contained on information systems and software applications that can communicate with each other, exchange data, and provide tools for using the information authenticated with the digital signature of the professional who provided the care. It is stored, updated, and used under strict conditions of security, integrity, authenticity, reliability, accuracy, intelligibility, conservation, availability, and access, in accordance with the regulations in force.
Main topics addressed in the regulation	Definition of the EHR/Scope of application/Interoperability/Implementation plan and deadlines/Role of public actors in implementing EHR (MINSAL, MINTIC, Archives)/Custody and safekeeping/Ownership/ Content, status as free, and authenticity of EHR/Information security/Funding/Handling the physical file.

Costa Rica

Regulation	**Law 9162** — Unified Digital Health Record.
Objective of the regulation	**Article 1.** The purpose of this law is to establish the scope and action mechanisms needed to undertake the process of planning, funding, supplying, resourcing, and implementing the unified digital health record countrywide.
Definition of EHR	The term unified digital health record is defined as a repository of patient data in digital format that is stored and exchanged securely and can be accessed by multiple authorized users. It contains retrospective, contemporaneous, and prospective information, and its main purpose is to support healthcare in an ongoing, efficient, quality, and comprehensive way.
Main topics addressed in the regulation	Definition of EHR/Scope of application/Guidelines for the technological solution, including those on interoperability, security, scalability, identification, single access, and other aspects/Implementation plan and the role of public actors/Funding/Corporate social responsibility/Protection and security of information.

Ecuador

Regulation	**Regulation 0009-2017** — The following regulation is issued for the management of electronic health records.
Objective of the regulation	**Article 1.** The purpose of this regulation is to order the implementation of the Electronic Health Record, as well as set out guidelines for its application at healthcare establishments nationwide.
Definition of EHR	The Electronic Health Record is a personal electronic record resulting from health care that is contained in a database created using computer programs and certified with the electronic signature of the health professional. Without prejudice to the fact that health care establishments are the custodians of the Electronic Health Record, patients are the owners of the data on them that is stored in the Electronic Health Record.
Main topics addressed in the regulation	Definition of EHR / Scope of application / Diversity of information systems / Role of the National Health Authority in determining content, use, and management / Role of establishments / Security, confidentiality / Content / Interoperability / Role of professionals and use of electronic signature / Transition provisions.

El Salvador

Regulation

Resolution 941 — Technical regulations on the composition, consultation, and custody of health records.

Objective of the regulation

Article 1. The purpose of this regulation is to establish the technical provisions governing the management of documents and the protection of data in the medical file and other documents related to the care provided to people at healthcare institutions and establishments.

Definition of EHR

The health file is the legal document to which essential and detailed data generated during the care provided to the user is added in an orderly fashion. It is considered an organized record of the healthcare process; it provides documentation in legal, administrative, and technical procedures for both users and healthcare personnel; and it is a primary source of information for epidemiological surveillance, clinical research, and teaching. The information must be logged by medical personnel, paramedics, or another party authorized by the relevant surveillance council and who provided the care; it is used to record health promotion, disease prevention, treatment, habilitation and rehabilitation actions, and its aim is to document a person's health status, diagnosis, treatment, and the progression of their disease. The file can be kept in physical or electronic format, or any other format that guarantees its authenticity, integrity, and conservation.

Main topics addressed in the regulation

As stated in Article 1, this law covers the medical file in general (whether physical or electronic), but Chapter IV contains key provisions on aspects specific to electronic medical files, such as: Cybersecurity/Backups/Access control/Identification and authentication/Protecting personal data, and others.

Mexico

Regulation

Official Mexican Standard NOM-024-SSA3-2010, which establishes the functional objectives and functionalities that the products of the Electronic Health Files Systems should have (...).

Objective of the regulation

Article 1. The purpose of this Official Mexican Standard is to establish the functional objectives and functionalities that products of the Electronic Medical Files Systems should have in order to guarantee the interoperability, processing, interpretation, confidentiality, and security of information in electronic health records, as well as the use of standards and catalogs for that information.

Definition of EHR

Electronic health file system: The electronic means by which health personnel must register, log, and certify the action they take in relation to the patient, in accordance with the health regulations. It enables unified management of a single, longitudinal health record for each patient in digital format.

Main topics addressed in the regulation

Definition of EHR/Scope of application/Interoperability and standards/Processing data/Security and confidentiality/Information and content/Identification and authentication/Functions and features of systems/Criteria for evaluating systems.

Peru

Regulation

Law No. 30024 — Law creating the National Registry of Electronic Health Records.

Objective of the regulation

Article 1. The purpose of this law is to create the National Registry of Electronic Health Records and establish its objectives, administration, organization, implementation, confidentiality, and accessibility.

Definition of EHR

Electronic health record: A unified, personal, and multimedia health record contained in an electronic database, logged using computer programs, and authenticated with the digital signature of the professional who provided the care. It is stored, updated, and used under strict conditions of security, comprehensiveness, authenticity, confidentiality, accuracy, intelligibility, conservation, availability, and access, in accordance with the regulations approved by the Ministry of Health as the entity with authority over the matter.

Main topics addressed in the regulation

Creation and definition of the National Registry of Electronic Health Records/Definition of EHR and key terms, including interoperability, standards, access, digital signature, and others/Objectives of the National Registry of Electronic Health Records/Administration and organization of the National Registry of Electronic Health Records/Implementation of the National Registry of Electronic Health Records/Confidentiality/Authentication of identity/General and transition provisions.

Uruguay

Regulation	**Decree 242/017** — On mechanisms for exchanging medical information for healthcare purposes using the national electronic health record system.
Objective of the regulation	**Article 1.** The purpose of this Decree is to govern aspects related to the electronic processing and exchange of personal information by public and private institutions with legal authority over health-related matters, as well as the National Electronic Health Records System and its Platform.
Definition of EHR	The Electronic Health Record is the comprehensive set of medical, social, and economic data on a person's health, from their birth until their death, processed using electronic means, being the functional equivalent of the paper medical file.
Main topics addressed in the regulation	Definition of EHR and other key terms like Electronic medical document, National Electronic Health Record Platform, and others/Scope of application/Principles of EHR in terms of purpose, reliability, completeness, confidentiality, information, accessibility/Authenticity and value as evidence/Security/ Control of access and modification/Systems and platform/Access to the platform/Exchanging information/Final provisions.

>> b) Category 2. Patient data protection and secondary use of information

This category, as mentioned in section 2, is the one that with the highest number of laws, decrees, and regulations in the countries covered in the study. More specifically, this category includes legislations that are primarily focused on *habeas data*[5] and that cover all sectors of the state, including institutions, individuals, and public-private spheres. These regulations, most of which are at least two decades old, address a broad spectrum of issues related to the protection of personal data, including its use and exchange. There are also countries where the traditional *habeas data* laws are complemented by regulations on protecting digital data in EHR. This section also analyzes the legal provisions related to security, storing data, and secondary use of information.

Countries with *habeas data* laws. The authors found that a numerous group of countries have general and broad regulations on protecting personal data, regardless of the medium, format, and subject matter, where health is included but is not addressed in a specific legislation (Argentina, Bahamas, Barbados, Belize, Bolivia, Brazil, Chile, Guatemala, Guyana, Honduras, Jamaica, Mexico, Panama, Paraguay, Peru, Nicaragua, Dominican Republic, and Trinidad and Tobago). These regulations govern the protection of sensitive data, which is defined as data that reveals people's racial and ethnic origin; political opinions; religious, philosophical, or moral convictions; or union membership, or information about their health or sexual activity. In these countries, the exchange of information at the national level is defined as sending information from the source to the health authority. Reasons for exchanging data include statistical purposes, recordkeeping, protecting the population's health, and granting benefits. But in most cases the legislation mentions that data is exchanged out in response to a specific request from public government agencies to the producers or owners of the information, making the availability of that data and the systematization of its integration a challenge.

Countries with *habeas data* regulations and specific regulations on protection of the EHR data. Another group of countries, citing the *habeas data* law, include paragraphs in their specific electronic health records legislation about personal data protection and public information exchange in electronic format (Colombia, Costa Rica, and Uruguay). By including these sections, these countries are taking a step to modernize and update the protection of personal data by addressing digital aspects, interoperability, and individuals' immediate access as owners of the data. In these cases, EHR information is exchanged because of the prior existence of a network of institutions between which information can be exchanged, with the relevant local particularities and restrictions. In the case of data protection, data in electronic format is already mentioned and has to do specifically with the issue of health and patient information.

Lying somewhere between the two previous groups, Ecuador and El Salvador have specific laws on protecting and exchanging health information that cover both physical and electronic formats. These laws specify the responsibilities of the state, of health professionals, and of individuals in handling the information in different levels of detail. In El Salvador, "*individuals or entities that wish to conduct research and for that reason request the use of and access to the medical file must have the approval of the Institutional Ethics Committee and sign a sworn statement affirming that they will protect the personal data and use the information in a way that guarantees the legal right to confidentiality and that the information will be used exclusively for research purposes.*"[6]

[5] Within the American hemisphere, some (but not all) national legal systems recognize a right of "*habeas data*," by which individuals are able to file a judicial proceeding to prevent or terminate an alleged abuse of their personal data. That right may provide the individual access to public or private data bases, the right to correct the data in question, to ensure that sensitive personal data remains confidential, and to rectify or remove damaging data. http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_documentos_referencia_CJI-doc_474-15_rev2.pdf

[6] Article 39. From El Salvador's technical regulations on the composition, consultation, and custody of medical records.

Data security and secondary use of information. Most of the countries coincide on the issue of security when storing patient data with varying degrees of detail. This dimension is closely related to the protection of personal data and refers specifically to the obligation of institutions, providers, or professionals to safeguard patients' data and health records. Some regulations specify the strategic or technical measures that should be taken. This is the case with Colombia, where "*stakeholders that process information under the rules in this section must make a plan for keeping the information private and secure, for digital security, and for continuity of service, to which end they shall create a strategy for conducting a periodic assessment of digital security risks, which includes an identification of improvements to be made to their Operational Risk Administration System.*" Other more general regulations establish the obligation of the data controller or user to guarantee security, without specifically indicating how to do so.

In terms of secondary use of data, while all countries that in some way regulate this matter do so by making the anonymity of sensitive data a mandatory condition, one group of countries establishes this condition in their *habeas data* laws[7] or other similar laws, and another specifically includes this issue in their EHR legislation. Another smaller group of countries specifically addresses the issue of secondary use in their health legislation. Honduras' health code, for example, grants the Secretariat of Health the power to authorize the use of this data: "*To request data or carry out procedures related to health research, all individuals or institutions must have prior authorization from THE SECRETARIAT, or the body delegated by THE SECRETARIAT.*"[8]

[7] The laws on personal data have different names. Examples include: Protection of Personal Data, in Colombia, and Protection of Private Life, in Chile.
[8] Regulation 65-91 Honduran Health Code.

>> c) Category 3. Actions of health professionals

The category for actions of health professionals covers all regulations on responsibilities related to accessing and handling patient data and information, on the legal validity of professionals' digital or electronic signature, and on the use of electronic prescriptions. Because they have to do with professional practice, in many countries these matters are governed by professional associations rather than national regulations.

Digital signature and electronic documents. Most countries in this study have an overarching law or regulation on the digital or electronic signature that gives them the same value as wet signatures, regardless of whether the signer is a public entity, private enterprise, or individual (Argentina, Barbados, Belize, Bolivia, Brazil, Costa Rica, Chile, El Salvador, Guatemala, Honduras, Jamaica, Nicaragua, Dominican Republic, Suriname, Trinidad and Tobago, and Venezuela). In these cases, digital signatures are unequivocally linked to electronic documents and the owner of the signature. Most of these countries distinguish between a digital or electronic signature, which is "*any sound, symbol, or electronic process that allows the recipient of an electronic document to at least formally identify its author,*"[9] and an advanced electronic or digital signature, which requires authentication from the national oversight mechanism, which may be a committee or institute.

There is a very close relationship between digital signatures and electronic or digital documents, which is comparable to the relationship between a handwritten signature and a paper document. It is thus usually clarified that both documents created using digital means and paper documents that have later been digitalized are considered electronic documents. This clarification is made to give documents that have been signed digitally or electronically subsequent value as evidence.

Countries with specific regulations on EHR as well as a general law on digital or electronic signatures have introduced regulations on the direct relationship between the digital signature and electronic health record. These regulations established that the professional who signs is person who completes the EHR and associated the authenticity of and responsibility for the data it contains with that professional (Colombia, Ecuador, Mexico, Peru, and Uruguay). In the case of Panama, which also emphasizes protecting patients' rights, the responsibility falls to the institutions that employ the professionals and health personnel: "*The administration or management of hospitals or health centers shall ensure proper use of patients' data files, instituting security, control, and registration measures any time the data is accessed.*"

Controlling health professionals' access to health data. Countries also differ in how they handle the restriction of the access of health professionals or personnel to patients' information. One group approaches the issue from the perspective of "access protection," focusing on the integrity and/or confidentiality of the information, as well as professional responsibility. These countries specify that if EHR has been implemented, steps should be taken to adopt the use of restricted accesses with passwords or other means of identification (Argentina, Brazil, Ecuador).

In the case of Costa Rica, the regulations extend to the responsibility of each user authorized to access the Unified Digital Health Record, and they provide further guidelines for developing security levels for accessing that record, specifying the limit associated with each user's access level.

When specifically addressing how personnel access medical records (without specifying the format), some countries place particular emphasis on logging information about opening, moving, and closing the medical file. This group

[9] Law 19799 on electronic documents, electronic signatures, and electronic signature authentication services.

specifies that professionals with no direct connection to a person's care do not have permission to access the records. Thus, health record access control systems should identify, when both opening and closing the document, details such as name, date, time, and changes made, which are required in the medical file log (Chile, Mexico, Peru, Uruguay, El Salvador).

For a larger group of countries, the matter of access restrictions is closely tied to Category 2 (protecting patient data and secondary use of information), since these countries include articles in their overarching data protection regulations on information technologies or security and access to information. Although these legal frameworks do not specifically mention health, they contain provisions for implementing technical and administrative controls that prevent, among other actions, unauthorized or fraudulent access to personal data (Bolivia, Paraguay, Dominican Republic, Barbados, Bahamas, Guyana, Jamaica, Venezuela, and Trinidad and Tobago).

Exceptions for emergencies, public health reasons, or epidemiological reasons are included in some regulations on accessing personal data (Argentina, Bahamas, Barbados, Brazil, Chile, Ecuador, Mexico, Dominican Republic, Trinidad and Tobago, and Uruguay). Colombia's regulations specify that data in health records can be accessed if requested via legal channels: "*Authorizing third parties. Only the Electronic Health Record's data subject shall be able to authorize third-party use of all or part of the information it contains in accordance with the regulations in force, with the exception of cases in which by law such authorization is not required.*"

Healthcare professionals and electronic prescriptions. Regulations on electronic prescriptions are in their beginning stages the region, having just started to emerge since the first months of 2020. This study includes this aspect in the category of actions of health professionals, since electronic prescriptions are viewed or defined as part of those professionals' domain in most countries. The aim of the legislation in one group of countries (Argentina, Brazil, Chile, Ecuador, and Panama) is to give professionals authority to issue prescriptions in electronic or digital form. For example, a paragraph from Argentina's law 27553 reads: "*This law applies to all prescriptions from doctors, dentists, or other health professionals who are legally authorized to give prescriptions in the different spheres of healthcare and public and private pharmaceutical care. Medications prescribed in electronic or digital prescriptions must be dispensed at any pharmacy in Argentina, by pharmacy services at health care establishments, and by health-sector establishments.*"

In Costa Rica, Mexico, and Peru, electronic prescriptions are directly tied to the technological development of a specific module in the EHR computer system. Within this group, Peru links electronic prescriptions to EHR and to telemedicine services, provided the Ministry of Health has authorized the professional to issue prescriptions: "*Electronic prescriptions are incorporated into telemedicine services and electronic health records as a technological tool enabling the use of ICT to communicate the prescription to patients, in compliance with the current regulations on guaranteeing the authenticity of the document. Electronic prescriptions are sent to the user via ICT and are legally valid for use at pharmacies and Health Insurance Fund Management Institutions (IAFAS in Spanish; Instituciones Administradoras de Fondos de Aseguramiento en Salud).*"

Uruguayan regulations focus on the prescription itself, as separate from professional practice or the institutions that issue or fill it. Its regulations specify how the prescription should be written: "*Electronic medical prescriptions are considered fully legitimate, valid, and effective, in accordance with Law No. 18600 of September 21, 2009, and they must contain the following information, at minimum: pharmaceutical form, dosage, route of administration, and concentration of the drug in question, identity of the prescriber, identity of the user, and how long the prescription is valid from the prescription's date of issue.*"

>> d) Category 4. Role of patients in relation to their health data

It is essential for the regulatory framework to recognize patients' rights in relation to their health data. Patient-centered healthcare systems should guarantee individuals' consent to use their data, ensure timely access to that data for patients and their ability to modify the data as provided for by law, and establish reliable identification and authentication mechanisms. This section covers these three topics.

Patient consent to use of their data. Most countries included in this study have laws on patient rights and consent when using their personal health data. These include Argentina, Brazil, Chile, Colombia, Costa Rica, Mexico, Panama, Peru, Uruguay, Bolivia, Nicaragua, Barbados, Dominican Republic, Bahamas, Jamaica, Venezuela, and Trinidad and Tobago.

Some countries' health laws have specific clauses about consent, which must be given previously (Argentina and Uruguay): "*when personal data is collected, the data subjects must first be clearly and explicitly informed*."[10] More generally, countries have clauses related to patient consent as part of more general data protection laws. These clauses allow people to withdraw their consent at any time (Bolivia, Costa Rica, and Barbados). Barbados, for example, allows patients to withdraw consent that had previously been granted. Its regulation states that "*A data subject has the right to withdraw his consent in respect of the processing of his personal data at any time and the data controller shall inform the data subject of his right to withdraw prior to him giving consent to the data controller to process his personal data. The withdrawal of consent by the data subject shall not affect the lawfulness of processing based on consent before its withdrawal*[11]."

Patient identification and authentication. Patient identification—the use of electronic identification means, such as assigning unique numbers or letters to each patient to protect their identity—was addressed by a smaller number of countries in the region. Some countries require a specific way of identifying patients, like creating a unique patient identification code, using numbers to replace their first and last names, automatically assigning a unique numbering, or using their identity card (Argentina, Panama, Ecuador, Brazil).[12] In Brazil, reasonable and available technical means must be used to anonymize patient-related data. In Mexico, the legislation provides detailed instructions on how to register a patient's identification and authentication: "*Information systems must use a federated authentication model based on the following rules: 5.5.1. System users must be authenticated with a Simple Electronic Signature, meaning a username of more than 6 characters, an alphanumeric identification password must include numbers, lowercase letters, and uppercase letters, and a second signature for signing electronic documents that must be different from the identification signature but follow the same rules.*"[13]

Access to data and editing rights. As explained in the previous section, more than 70% of the countries in the study have laws that guarantee the right to access and edit personal data (Argentina, Brazil, Chile, Colombia, Costa Rica, Ecuador, Mexico, Panama, Peru, Uruguay, Bolivia, Nicaragua, Barbados, Dominican Republic, Bahamas, Guyana, Jamaica, and Trinidad and Tobago). Countries with specific legislation on EHR included articles on patients' access to their personal health data. Other countries, like Costa Rica and Ecuador, have specific laws to ensure that patients can access their health data in general,[14] regardless of whether it is in a medical file. A larger group of countries addresses

[10] Article 6 of Argentina's Law 25326.
[11] Data Protection Act, 2019, Barbados.
[12] Argentina, Law 26529; Panama, Executive Decree No. 1458; Ecuador, Regulation on Confidential Information in the National Health System—patients' names and surnames must be replaced by their identity card number, and Brazil, Rule No. 2073.
[13] NOM-024-SSA3-2012, from Mexico.
[14] Costa Rica - Law on protecting people when processing their personal data/Law 8239 on the rights and duties of individual users of public and private health services, and Ecuador — Regulations on confidential information in the national health system.

accessing and editing personal data in general, which, based on the nature of the legislation, covers all confidential personal data controlled by the public sector, including health data. In this case, the overarching laws are the data protection or information access laws analyzed in category 2.

In terms of editing data, certain legislations differ notably on whether it is possible to "eliminate," "erase" or "delete" patient information. This option is expressly authorized in certain legislations[15] (Argentina, Chile, Colombia, Costa Rica, Mexico, Uruguay, Bolivia, Nicaragua, or the Dominican Republic), while others only allow data to be "modified" (Brazil, Peru, Guyana, or Jamaica).

It is important to highlight the conditions for editing data, as some countries, like Peru, allow editing when the recorded data is incomplete or wrong, while others specify no preconditions for editing. Only few countries addressed what happens to previous versions of modified data. Uruguay specifies that "*new data shall be added with the date, time, and electronic signature of the person who made the correction, without erasing the version that was corrected*."[16]

[14] Some countries specifically used the term "eliminate" while others used "deletion" of data, but we treat both as the "elimination of data."
[15] Decree No. 242/017. Uruguay

>> e) Category 5. Standards for health and interoperability of EHR

The region's different national regulatory frameworks also have distinct formulas and configurations with respect to the use of standards for health and the interoperability of EHR. As mentioned previously, this is one of the least-developed categories in the region. The countries that have made some progress on the issue can be put into three groups.

Countries that address interoperability in a generic way. The first group of countries has addressed the issue of interoperability in the public sector in a generic way, without specifically referring to the health sector and its unique characteristics. These countries have general regulations on, for example, digitalizing the public sector, which address the issue of interoperability in one or more provisions. In Bolivia, article 19 of Supreme Decree 2514 establishes the responsibilities of the government agency in charge of coordinating actions for interoperability in the context of electronic government, stating that "*the body overseeing electronic government shall establish the general policy and specific regulations for interoperability and the exchange of information and data between public sector entities*."

Countries that address interoperability in the health sector. A second group of countries has approved regulations on interoperability with specific references to the health sector and EHR, without mentioning the standards to be used or specifying the steps to be taken to ensure the interoperability of health systems and processes. In other words, the countries in this group declare the need for interoperability between systems, but they do not lay out the path to achieving it. For example, article 2 of Law 2015 of Colombia defines interoperability as the "*capability of various systems or components to exchange information, understand this data, and use it*" in order to ensure the "*system-wide consistency and quality of the data, with the resulting benefit in terms of continuity of care and safety for patients.*" Countries like Panama are also part of this group.

Countries that specify the use of interoperability standards in health. A third group of countries took an additional step and more precisely defined how EHR interoperability will be achieved. The countries in this group defined the type of standards and terminology to be used to guarantee the exchange of data between health information systems. These details are usually set out in the technical appendices to the texts of the regulations. Argentina, for example, proposes a series of standards to be used in the appendix to Resolution 680/2018, which states that "*SNOMED is proposed as the terminology for recording information in medical documents, and HL7 standards are proposed for structuring and communicating information (CDA and FHIR). CIE-10/CIE-11 are proposed as standards for statistical analysis in the field of health*." Similar appendices are found in the regulatory frameworks of Brazil (Appendix to *portaria* 2073), Mexico (NOM-024-SSA3-2010), or Uruguay (Appendix to Decree 122/019), for example.

Costa Rica took a more flexible approach to defining and using standards in the area of health. In its Regulations on the "*use of standards for health data in caring for patients*" (No. 39652-S-MICIT), instead of naming the standards to be used, the country decided to create the National Health Data Standardization Committee (article 2), which is in charge of: defining ontologies, terminologies, and classifications for health; defining a health information architecture; periodically updating the rules and standards for transferring health data; and enabling functional, syntactical, and semantic interoperability (article 3). This approach seems to provide a clear path to interoperability, allowing a certain level of flexibility to adapt to constantly changing terminology and standards.

Lastly, it should be noted that the issues surrounding EHR interoperability are closely tied to the dimensions examined in other categories of the conceptual framework, such as, for example, clearly defining a minimum dataset to be exchanged (Category 1) or legal provisions on exchanging health information at the national level (Category 2).

Section 4: Conclusions and recommendations

The analysis of studies and specialized literature reveals a certain level of consensus about key dimensions to be included in legal framework for implementing EHR. This consensus was used to develop a conceptual reference framework to organize the search and identify and analyze the legislation in 26 countries in the region. An analysis of over 115 legal texts compiled from the legislative portals of the countries included in the study and other complementary sources yields a series of conclusions and recommendations for strengthening the existing legal frameworks in the region.

CONCLUSIONS

The region has made mixed progress towards developing regulatory frameworks for implementing EHR at the national level. Of the countries analyzed, 10 have regulatory frameworks that address more than 75% of the essential dimensions in the conceptual framework, and 7 countries address between 50 and 75% of these dimensions. These frameworks include some regulations on specific aspects of EHR, as well as those on data protection, the actions of health professionals, the role of patients, and interoperability. The other countries have regulatory frameworks that cover less than 50% of the key dimensions in the conceptual framework. All of the countries analyzed have made basic progress on one or more categories, which can be a starting point for developing a strong regulatory framework for implementing EHR.

The least-developed category is "Specific aspects of EHR." There is a region-wide lack of frameworks for developing these systems. The category for interoperability and using standards for exchanging medical data is also underdeveloped. At the regional level, only 31% of countries have specific regulations for implementing EHR, only 31% mention codes and standards for interoperability, and just 19% specify the minimum dataset to be exchanged in EHR.

88% of countries in the region have regulations on protecting health data. This level of progress is largely due to the inclusion of this matter in *habeas data* and personal data protection regulations, which address any case of handling of data in any format. However, most of these regulations were approved last century, so they do not cover specific issues like the exchange and interoperability of health data.

While it is not possible to infer causality, there seems to be a correlation between the countries that have made the most progress in implementing EHR systems and their regulatory progress, especially on specific aspects of EHR. A regional analysis shows that countries in the region that developed specific regulations for implementing EHR at the national level included provisions on: **i)** the definition of EHR, its purposes, functions, and features; **ii)** the guiding principles of EHR in terms of purpose, reliability, completeness, confidentiality, information, accessibility, and ownership; **iii)** the scope of

application; **iv)** the type of information and content to be exchanged; **v)** interoperability and standards; **vi)** data protection, security, and confidentiality; **vii)** safeguarding and custody of the information; **viii)** access and identifying and authenticating users; **ix)** the implementation plan and timeframe; **x)** managing files and transitioning from paper to digital format; **xi)** the role of public, private, and professional stakeholders, as well as users, and **xii)** funding. These specific regulations often reference and form a harmonious part of a broader regulatory framework consisting of laws on *habeas data*, on the rights and responsibility of patients and health professionals, on electronic signatures and documents, and others.

There is no single magic recipe for regulatory frameworks. Rather, the many local experiences represent a wide variety of formulas and different ways of incorporating the different dimensions. This diversity can be most obviously seen in the various ways of referring to EHR in the different national contexts. But beyond lexical considerations, the several definitions emphasize different characteristics of EHR. This diversity can be found in each dimension of the conceptual framework: some countries are more specific than others about the type of information to be exchanged; some are more permissive than others in relation to patients' rights to modify and edit their data; different countries have different ways of handling patient identification and health professionals' rights to access health data; and they go into varying degrees of detail on using and updating interoperability standards. The countries' different levels of progress and the wide variety of regulatory formulas creates an important opportunity for countries to exchange experiences and lessons learned.

This document is a first step towards a systematic survey of regulations on digital health. This survey encompasses regulations that go beyond EHR in the strict sense and in the future will go into more depth in other spheres such as, for example, telemedicine, using artificial intelligence in health, regulatory aspects related to cloud computing, and others.

RECOMMENDATIONS

- Countries need to develop specific regulations on EHR to encourage its implementation at the national level. **These regulations should ideally cover: i)** the definition of EHR, its purposes, functions, and features; **ii)** the guiding principles of EHR in terms of purpose, reliability, completeness, confidentiality, information, accessibility, and ownership; **iii)** the scope of application; **iv)** the type of information and content to be exchanged; **v)** interoperability and standards; **vi)** data protection, security, and confidentiality; vii) safeguarding and custody of the information; **viii)** access and identifying and authenticating users; **ix)** the implementation plan and timeframe; **x)** managing files and transitioning from paper to digital format; **xi)** the role of public, private, and professional stakeholders, as well as users, and **xii)** funding.

- In addition to mapping out the existing dimensions, more detailed maturity analyses need to be conducted to identify specific areas for improvement in the different countries. The next step after this analysis is studying the quality of the legal content in more detail, identifying possible areas that need to be developed further or addressed more specifically, and, in certain cases, identifying and correcting possible contradictions and inconsistencies between legal texts in the regulatory framework.

- The progress made on health data interoperability needs to be developed further, establishing regulations that promote the use of standards and clearly define the type of data and information to be exchanged. Countries that have successfully implemented EHR systems created appendices, regulations, and technical guidelines that identify variables, specify how they are coded, and state whether their exchange is mandatory or optional, and other aspects. This has allowed them to standardize and optimize the processes of exchanging information and ensure that people's health data can move fluidly in a protected and secure environment.

- With regards to data protection, *habeas data* and personal data protection laws need to be updated to cover digital concepts and issues as most of them were passed before the digital era. While this analysis underscored the significant progress made on protecting health data, which was the best-developed category in the conceptual framework, these legal texts do not necessarily fully capture the possible threats to personal health data in the digital era. Likewise, outdated regulations can make it difficult to share health data between the ecosystem's different stakeholders in a protected way.

- In addition to laws, countries need to develop and approve technical guidelines that provide more clarity and detail on putting the legal provisions into practice. Laws and their regulations usually specify *what* must be done in the different categories in this study, but they are not necessarily the place to go into detail on *how* to do so. To implement patient identification, digital signatures and documents, or exchanges of data, the question of how these aspects will be implemented needs to be clarified through technical standards that complement the legal framework. Without these technical standards and good change management to encourage their adoption, countries run the risk that legal provisions will end up being a paper exercise and never materialize in practice.

- Lastly, it is necessary to foster an exchange of experiences and lessons learned among countries. It is important to constantly learn from the successes, but also from the difficulties faced by the other countries in the region. While there is no magic formula, and each country must develop regulations suited to its specific situation. Countries also need to identify best practices and keys to success, properly document them, and share them. This will certainly help many countries in the region more swiftly close the gaps that were identified and more fully tap into the digital era's immense opportunities for health.

Acknowledgment

The authors would like to thank Ferdinando Regalia, Luis Tejerina, Jennifer Nelson, Mario Casco, Marcelo D'Agostino, Pablo Orefice, Fernando Portilla, Daniel Otzoy, Guillermo Schor-Landman and Marisa Aizenberg for their valuable comments to this document.

References

- Appari, A., & Johnson, E. (2010). Information Security and Privacy in Healthcare: Current State of Research. *International Journal of Internet and Enterprise Management*. 6(4): 279-314. https://doi.org/10.1504/ijiem.2010.035624

- Inter-American Development Bank, Red americana de cooperación sobre salud electrónica. (2019). *Modelo Institucional y normativo para implementar salud electrónica: Recomendaciones técnicas*. IADB. https://socialdigital.iadb.org/es/resources/health/kits-de-herramientas/271/273

- Borbolla, D., Becerra- Posada, F., & Novillo-Ortiz, D. (2019). Marco legal para registros médicos electrónicos en la Región de las Américas: definición de dominios a legislar y análisis de situación. *Revista Panamericana de Salud Pública*. 43/e25.

- Carnicero, J., & Serra, P. (2020). *Gobernanza de la salud digital: El arte de la transformación de los sistemas de salud*. Inter-American Development Bank. http://dx.doi.org/10.18235/0002661.

- EU Health Programme. (2014). *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services.* https://ec.europa.eu/health/sites/health/files/ehealth/docs/laws_report_recommendations_en.pdf

- Hiller, J., McMullen, M., Chumney, W.M., & Baumer, D. (2011). *Privacy and Security in the Implementation of Health Information Technology (Electronic Health Records): U.S. and EU Compared*. http://hdl.handle.net/10919/80420

- Hoffman, S., & Podgurski, A. (2013). Big Bad Data: Law, Public Health, and Biomedical Databases. *The Journal of Law, Medicine & Ethics, 41*(1_suppl), 56–60. https://doi.org/10.1111/jlme.12040

- Hoffman, S., & Podgurski, A. (2008). *Finding a Cure: The Case for Regulation and Oversight of Electronic Health Record Systems.* (2008). Case Western Reserve University School of Law. Faculty Publications. 1. https://scholarlycommons.law.case.edu/faculty_publications/1

- International Organization for Standardization. (2014). *Health informatics – Capacity based eHealth architecture roadmap- Part 2: Architectural components and maturity model* (ISO/TR 14639-2:2014). Retrieved from https://www.iso.org/standard/54903.html

- Nelson, J., Tejerina, L., & Cafagna, G. (2020). *Sistemas de Historias Clínicas Electrónicas: Definiciones, evidencia y recomendaciones prácticas para América Latina y el Caribe*. Inter-American Development Bank. http://dx.doi.org/10.18235/0002240

- World Health Organization. (2012). *Legal frameworks for eHealth*. WHO Press. https://www.who.int/goe/publications/legal_framework_web.pdf

- World Health Organization. (2016). *Atlas of eHealth country profiles: The use of eHealth in support of universal health coverage- Based on the findings of the third global survey on eHealth 2015*. WHO Press. https://apps.who.int/iris/bitstream/handle/10665/204523/9789241565219_eng.pdf;jsessionid=9FA7B50FECD8B-82DA00D1085E6975FE0?sequence=1

- Pan American Health Organization (2020). *Estrategia y Plan de acción sobre eSalud (2012-2017)*. Retrieved from https://www.paho.org/ict4health/index.php?option=com_content&view=article&id=54:estrategia-y-plan-de-accion-sobre-esalud-2012-2017&Itemid=146&lang=es

- Pan American Health Organization (2020). *Registros electrónicos de salud e interoperabilidad: dos conceptos fundamentales para mejorar la respuesta de salud pública*. Pan American Health Organization. https://iris.paho.org/handle/10665.2/52004

- Silcox, C. (2020). *La inteligencia artificial en el sector salud: promesas y desafíos*. Inter-American Development Bank. http://dx.doi.org/10.18235/0002845

- Terry, N., & Francis, L. (2007). Ensuring the Privacy and Confidentiality of Electronic Health Records. *University of Illinois Law Review*, 2007, 681-735.