Information Security

Policy Overview

Eight Guiding Principles for the Digital Transformation of the Health Sector

Digital transformation toolbox

PAHO Pan American Health Organization World Health Organization Americas

ORGANIZATION, COORDINATION, AND DEVELOPMENT

Department of Evidence and Intelligence for Action in Health (EIH) of the Pan American Health Organization (PAHO), in collaboration with the Center for Implementation and Innovation in Health Policy (CIIPS), part of the Institute for Clinical and Health Effectiveness (IECS) of Argentina, a PAHO collaborating center.

ACKNOWLEDGEMENTS

PAHO wishes to express its gratitude to the Government of the United States of America for the financial contribution that made possible the development of this important product, which is part of a toolbox to support the strengthening of the implementation of the regional telehealth initiative in the fight against noncommunicable diseases.

PAHO recognizes and appreciates the support of the Spanish Agency for International Development Cooperation (AECID), the United States Agency for International Development (USAID), the Government of Canada, the Inter-American Development Bank (IDB), and the network of experts who support the PAHO Information Systems for Health (IS4H) initiative.

Contents

01 Abstract

02 Introduction

04 Current status and identification of gaps

06 Lines of action

09 Monitoring indicators

11 General recommendations

12 References

Abstract

Information security is one of the eight guiding principles for the digital transformation of the health sector promoted by the Pan American Health Organization (PAHO). This policy brief presents key concepts, recommended lines of action, and monitoring indicators, with the objective of advancing information security.

According to the PAHO definition, this principle aims to **establish mechanisms for trust and information security in the digital environment of public health,** and to "adopt regulatory instruments for the treatment and protection of sensitive health data, as well as international security guidelines and standards for patient-centered information systems. Implementation of these systems must respect health-related rights in order to generate a 'culture of safe and reliable data management', understood as the balance between the need to access data and the need for privacy"*(1)*.

In the context of health, the information to be protected is not only a good, but also involves ethical, legal, and technical dimensions that must be safeguarded. The security of such data is defined in terms of the International Organization for Standardization (ISO) standard as preservation of "the confidentiality, integrity, and availability of information". This definition provides the three crucial elements that security mechanisms must consider to be useful to the organizations where they are implemented.

Information security, considered a cornerstone of the successful performance of any organization, institution, or system, encompasses the strategies, planning, and development that are carried out to protect information from the risk of attacks that would enable the improper or illegal use of the asset in custody.

This policy brief reviews the current state of information security, and provides recommendations, lines of action, and monitoring indicators. It is important to focus on an action plan that considers the following as essential aspects of its effectiveness: a security and data protection plan enshrined in public policies and in accordance with the law; a control structure for managing the flow of health information, including guidelines on computer security and associated risks; monitoring mechanisms aimed at detecting incidents; a procedure for handling informed consent files; centralized security certifications; and the promotion and development of plans for continuous training and staff development.

Moreover, regulatory instruments for protecting sensitive data in the area of health, and international guidelines on the security of health information systems, are needed to promote the proper use of data to strike a balance between access and privacy.

Keywords: security, ethics, accessibility, confidentiality, sensitive data, regulations.

Introduction

"It is imperative to protect sensitive health information, and therefore it is necessary to collaborate and co-create mechanisms for ensuring the confidentiality and security of personal information in the digital public health setting, while simultaneously promoting access and transparency in information and knowledge." Pan American Health Organization (PAHO) statement during the High-Level Conference on Information Systems for Health, February 2021.

Thinking about information security means taking into account what information is made available, by what means, to whom, where it is hosted, how that data is processed, what are its governing regulations and regulatory frameworks (or whether it is necessary to create them), and how to promote settings and circuits in which health rights are respected, while also facing the challenge of providing fluid and transparent data access while ensuring the confidentiality and privacy of sensitive information, such as that resulting from linking individuals to the health system.

The challenges that come with the search for robust strategies and a balance between the need to access health information while also considering the special privacy and security issues inherent to sensitive data invite us to consider several dimensions when addressing the principle of information security.

Besides adopting regulatory instruments on the treatment and protection of sensitive health data, it is important to be familiar with and to implement international security guidelines and standards for patient-centered information systems and focus on their most specific aspects in jurisdictional scenarios, not limited exclusively to a technical dimension, but creating and strengthening a path towards a culture of secure and reliable data management.

Digital technologies can contribute to increasing the most vulnerable population groups' access to health; however, it is also necessary to develop human capital and infrastructure that enable the inclusive, ethical and secure use of these technologies. Here, information security is a central principle.

A comprehensive approach to and review of information security encompasses establishing trust mechanisms in the digital environment of public health, considering ethical, technical, and legal dimensions.

Based on the consideration of information as an essential asset for these activities and the need for adequate protection, it is appropriate to emphasize, first, that health data are considered sensitive information; the writ of *habeas data* enables people to know what personal data of theirs are stored and used by third parties, and opt for the possibility of updating, amending, or deleting them. For example, in Argentina, the national legal framework considers that data use is mentioned in the Constitution, and that there is a set of laws specifically addressing personal data protection, patients' rights in relation to health professionals and institutions, and access to public information.

The World Health Organization (WHO) has published guidelines on aspects of digital health and cybersecurity, the development of interoperable health ecosystems, and the elaboration of legal requirements that guarantee ethical codes to safeguard the safety of patients and the security of their data. The European Union Agency for Cybersecurity (ENISA) has published warnings and recommendations on good practices in information security, especially regarding threat trends *(2)*. The Ibero-American Data Protection Network (RIPD) seeks to promote the regulatory developments and policies necessary to guarantee the advanced regulation of the right to personal data protection *(3)*. International Organization for Standardization (ISO) standards also establish the necessary controls and strategies to eliminate or minimize risks *(4)*.

Considering successful experiences and models that could serve to advance implementation, three dimensions and necessary conditions are highlighted:

- Defining an information security policy for the different stakeholders or organizations.

- Guaranteeing the coexistence of the different areas in a single network.

- Creating a regulatory framework that regulates the application of and compliance with regulations by the intervening parties that participate or wish to participate in the network.

Success in the execution of these lines of action is linked to clearly defining the proper procedures and establishing objectives, with the endorsement and active participation of the many stakeholders involved, in a cohesive and coordinated manner.

Current status and identification of gaps

The first aspect to be highlighted is the heterogeneity of existing regulatory frameworks in the countries of the Region of the Americas. There are different stages of normative development *(5)*: Colombia and Venezuela mention this subject in their constitutional frameworks; other countries, including Argentina, Brazil, Chile, Peru, Paraguay, and Uruguay, have specific laws on the processing of personal data.

PAHO urges each country to identify its need to develop regulations, seeking a balance between accessibility and privacy and aiming to protect the individual, without delaying or blocking the development of digital health technologies *(1)*.

International guidelines can serve as references and guides. However, it is desirable for countries to create their own frameworks, reflected in national strategies, as a complement to international standards and guidelines on data protection. Specific difficulties can be seen in some countries that are linked to such issues as the lack of mechanisms guaranteeing data security, the existence of jurisdictional differences regarding regulations, and the lack of international agreements on standards.

Secondly, it is necessary to develop policies for a security and protection plan for health data, focusing on access profiles based on the actions to be taken by the user.

Regarding this issue, the **changing data security environment poses another difficulty, as does the lack of information (in terms of figures and reporting on cybersecurity incidents in the Region).** This type of analysis and monitoring has existed in the European Union since the establishment of ENISA *(2)*, which provides up-to-date information on threat trends, helping stakeholders to recognize them and develop response strategies. ENISA also provides an overview of threats to systems, threat actors, and their current and emerging trends. This type of information is not yet available in the Latin American Region.

Thirdly, there is a **weak development of training strategies, aimed at stakeholders involved in the flow of health information, that address computer security guidelines and associated risks.** Such strategies would strengthen the training of specialized human resources able to resolve security incidents, and encourage the recognition of General Data Protection Laws (*5*) as initial instruments for promoting discussion on personal and organizational responsibilities. A set of RIPD recommendations was published to provide a reference model for future regulation in the Region, and for reviewing current regulations on the right to data protection in countries that do not yet have regulatory frameworks, or that need to update their existing laws *(3)*.

Moreover, **there are still no monitoring mechanisms to detect security incidents in health information systems.** Given this situation, it is necessary to strengthen national cybersecurity strategies. In this area, ISO standards provide the main reference (*4*); however, although ISO defines the controls and strategies necessary to eliminate or minimize risks, its standards are not adapted to local contexts.

Finally, the **public is still insufficiently aware of its rights and responsibilities regarding personal data, and of the need to have established procedures for informed consent regarding the access to and storage and safeguarding of sensitive information.** For example, in Argentina, Law 26,5296, enacted in 2009, establishes patients' essential rights in their relationship with health professionals and institutions, health insurance agents, and any other stakeholders.

Confidentiality is another issue addressed in legislation, insofar as patients have the right for any person who participates in the preparation or manipulation of their clinical documents, or has access to their content, to duly keep this information confidential, unless expressly provided otherwise by the competent judicial authorities or patients' authorization. Examples include two personal data protection laws: Organic Law 459 of Ecuador, from 2021(*6*), and Law 1,581 of Colombia, from 2012 *(7)*.

However, **the role of the patients as data subjects, and encouraging their active participation in the principle of data security, remains a challenge.** Users have yet to take on board their right to demand the protection of their information, the correct applications of data protection, and the continuity and robustness of the precautionary monitoring of anomalies.

Lines of action

PAHO proposes information security as one of the eight guiding principles of the digital transformation of the health sector *(1, 8, 9)*, including the following lines of action:

1. Create legal instruments that regulate the processing of and access to health data, based on the pillars of privacy, confidentiality, and information security.

2. Formulate public policies that incorporate a security and protection plan for health data, defining access profiles based on the actions to be taken by the user.

3. Actively train all stakeholders involved in the flow of health information on computer security guidelines and associated risks.

4. Coordinate monitoring mechanisms to detect security incidents in health information systems.

5. Determine procedures for informed consent regarding access to and storage and safeguarding of sensitive information.

6. Create centralized security certification services for sensitive health data, using such technologies as blockchain certification.

7. Adopt communication plans to raise public awareness regarding peoples' rights and responsibilities regarding their personal data.

8. Update existing data protection regulations (many of which were created before the digital age), including new topics such as cybersecurity.

Taking into account the complexity of achieving information security, the recommended lines of action cover technical, legal, planning, and management aspects, involving organizations and governments. Considering security from the beginning, breaking the pattern of only addressing security owing to risks or failures, or only during subsequent planning and implementation stages, will make everything more organized, scalable, and efficient, both at the institutional level when planning information flows, and at the governmental level to create a scenario as solid as possible.

The following are some recommendations that complement the lines of action established by PAHO in its Eight Guiding Principles for Digital Transformation of the Health Sector, which are useful for different stakeholders involved in information security, from institutions to government agencies.

1. CREATE LEGAL INSTRUMENTS THAT REGULATE THE PROCESSING OF AND ACCESS TO HEALTH DATA, BASED ON THE PILLARS OF PRIVACY, CONFIDENTIALITY, AND INFORMATION SECURITY

- Evaluate and define a regulatory framework that establishes the rules to be applied to network participants, which clearly establishes minimum compliance guidelines, and clearly details the sanctions or penalties to which the different stakeholders or organizations could be exposed regarding data access, based on the pillars of privacy, confidentiality, and information security.

2. DEVELOP A CONTROL STRUCTURE FOR THE FLOW OF INFORMATION IN HEALTH, INCLUDING GUIDELINES ON COMPUTER SECURITY AND ASSOCIATED RISKS

- Create audit mechanisms that enable regular control of the different bodies participating in the network to ensure that they comply with the rules applicable to network participants.

3. ESTABLISH MONITORING MECHANISMS AIMED AT DETECTING INCIDENTS AND VERIFYING COMPLIANCE WITH THE STANDARDS AND CONDITIONS FOR INFORMATION ACCESS AND TREATMENT

- Define a contingency plan and an operating plan for an emergency coordination unit in the telematic network to manage any security incidents that may arise, and to alert the network participants so that they can preventively or correctively neutralize these threats. This unit should act as an information repository on such incidents and disseminate the defense tools and techniques to be applied within the network.

4. DETERMINE THE TOOLS AND PROCEDURES FOR INFORMED CONSENT REGARDING THE STORAGE AND SAFEGUARDING OF SENSITIVE INFORMATION

- Consider the characteristics of the platforms and access interfaces and the availability of information, and frame them in a circuit that involves a formal commitment and the signing of informed consent forms and confidentiality agreements with which users must comply before accessing consolidated information.

- Monitoring and follow-up of these accesses, and their respective validations, is also recommended.

5. CENTRALIZE SECURITY CERTIFICATIONS

- Create services that enable centralized management of aspects inherent to the certification of sensitive health data using blockchain certification technologies.

- Generate mechanisms to enable updating of the regulatory framework to address new technologies or blind spots not previously considered, ensuring compliance with security standards.

6. DEVELOP AND IMPLEMENT COMMUNICATION AND TRAINING PLANS ON RIGHTS AND RESPONSIBILITIES REGARDING PERSONAL DATA

- Develop documents and spaces for training, dissemination, and awareness to proactively transmit knowledge about the current legal framework. Stakeholders' awareness of their rights and obligations is crucial: technical or circuit robustness is useless without the support of formal definitions regarding the rights, obligations, ground rules, and good practices that must be considered by the people and institutions involved in the information life cycle.

- At the governmental level, make explicit the rights of each person regarding their information and the obligations of institutions to treat it correctly. This must be an issue on the agenda.

7. UPDATE CURRENT RULES AND TOOLS RELATED TO DATA PROTECTION

- The emergence of new technologies and complex scenarios requires us to bear in mind that we are not facing static situations; rather, it is necessary to be able to generate cycles of continuous improvement and updating of technical, normative, and ethical dimensions so that they can integrate all the new elements falling under the principle of security. Defining a series of measures or static planning are not enough; situations that were not previously considered must also be addressed, continuously adjusting and monitoring the processes involved.

- In the case of governments, review the validity or expiration of the regulations that affect data circuits to amend or promote the creation of or adherence to new regulatory frameworks.

8. STRENGTHEN INTRA- AND INTER-INSTITUTIONAL COORDINATION

- Coordination is another central point. From an internal perspective, at the institutional level, information security is a cohesive element integrated with the other guiding principles of digital transformation in health. If several areas are involved within an organization, cohesion must be fostered in terms of how to deal with loading, storage, requests, and circuits for availability. From an external perspective, it is necessary to know the local, national, and international scenario in which information security is framed for correct compliance with and consideration of the prerequisites and obligations that must be met.

- The creation of working spaces and groups with other institutions and areas of government makes it possible to strengthen agreements, and government initiatives are recommended to convene public bodies that deal with information to deepen the security dimension, because those in the health field represent a particular case due to the characteristics of the data they use.

9. DEFINE CLEAR RULES REGARDING THE FLOW OF INFORMATION: LOADING AND AVAILABILITY

- Regarding the loading and characteristics of health data, an important call to action refers to achieving a univocal reference for user identity and the creation of authorization credentials and profiles for the use of and access to information systems, proactively training the stakeholders involved about guidelines on computer security, the associated risks, and the quality of the data being entered.

- The characteristics of these pieces of information, or raw data, that are uploaded must be thoroughly analyzed (level of aggregation, nominalization, content sensitivity) before defining who can access the data, in what format, and by what means or platform. It is likely that prior data processing will be necessary, to anonymize and eliminate the possibility of indirect identifiers.

Monitoring indicators

To advance in the development and implementation of health information security, the following indicators are proposed. It is important to clarify that this is not an exhaustive list, but that each country or region can incorporate other indicators, define the necessary level of disaggregation and frequency of measurement.

CROSS-CUTTING INDICATORS OF THE EIGHT GUIDING PRINCIPLES FOR DIGITAL TRANSFORMATION IN HEALTH

- A national digital health strategy established through a regulatory framework
- A governmental organization structure for leading the digital transformation strategy in health
- A budget for a digital agenda that includes human resources and the necessary technology

SPECIFIC INFORMATION SECURITY INDICATORS

Identifying indicators for information security surveillance is key to monitoring it smoothly and effectively, and verifying that the conditions guaranteeing correct data storage, access, and processing of data are met or properly adjusted.

Procedures for monitoring personal data protection require organized and coordinated elements, including alerts to potential risks and dealing with security incidents that could threaten user information. It is recommended that such procedures be planned and developed at the same time as the strategy for implementing health information systems, and not be mere adaptations to the characteristics of each system. These procedures must constitute a main element in the planning, to promote a structure and organization able to positively influence the solidity and robustness of the information security strategy.

Listed below are recommendations and suggestions related to the core issues of monitoring, privacy, confidentiality, security, and compliance.

1. Create legal instruments that regulate the processing of and access to health data, based on the pillars of privacy, confidentiality, and information security

- A regulatory framework that establishes the guidelines for compliance with confidentiality, privacy, and information security, as well as sanctions or penalties
- A mechanism for monitoring the regulatory framework with a certain frequency to enable identification of flaws and omissions, indicating needs for amendment and regulating aspects not considered previously

2. Develop a control structure for managing the flow of health information, including guidelines on computer security and associated risks

- A governmental body responsible for ensuring cybersecurity in the health sector and coordinating emergencies in the telematic network
- Defined circuits for monitoring and addressing incidents

3. Establish monitoring mechanisms aimed at detecting incidents, as well as verifying correct compliance with the standards and conditions for information access and treatment

- A defined monitoring strategy for tracking the activity of network users

- An incident information repository

4. Determine tools and procedures for informed consent regarding the storage and safeguarding of sensitive information

- Number of confidentiality agreements signed between the parties
- Number of informed consent forms signed

5. Centralize security certifications

- Number of services created that enable centralized management of the certification of sensitive health data through the use of blockchain certification technologies

6. Develop and implement communication and training plans on rights and responsibilities regarding personal data

- Number of documents disseminated on rights and responsibilities regarding personal data
- Space for training on rights and responsibilities regarding personal data
- Dissemination and awareness campaigns to proactively transmit knowledge about the current legal framework

7. Update current rules and tools related to data protection

- Strategy for updating the defined regulations

8. Strengthen intra- and inter-institutional coordination

- Working spaces and groups involving different institutions and areas of government, including users

9. Define clear rules regarding the flow of information: loading and availability

- A univocal reference for user identity and the creation of authorization credentials and profiles for using and accessing systems
- Number of stakeholder trainings about guidelines on computer security, associated risks, and the quality of the data being entered

General recommendations

Without underestimating the technical dimension, it is essential that, when developing their information security policies, decision-makers consider the following aspects:

- The role of patients as data subjects, and their active participation in the principle of information security
- The need for a comprehensive, cross-cutting, multidisciplinary approach addressing specific roles within organizations
- Emphasis on dissemination and awareness so that the different network stakeholders are aware of the current legal framework
- The importance of guaranteeing data integrity and availability to the different stakeholders in the network
- The development of appropriate regulatory frameworks, because although there are agreements and consensus around the normative references, it is worth highlighting the advisability of countries' generating their own national or local frameworks that contemplate the particularities of the circuits and systems involved
- The sensitive nature of the data resulting from people's interactions with the health field requires the development of tools, platforms, and strategies designed specifically to include the correct identification of those who intervene and participate

It is recommended that comprehensive strategies be developed to facilitate and encourage the use of data in as many positive actions as possible without compromising the security and rights of the data subjects.

References

1. Pan American Health Organization (2021). Eight Guiding Principles for Digital Transformation of the Health Sector: A Call to Pan American Action. Washington, D.C.: PAHO. Available at: https://iris.paho.org/handle/10665.2/54256.19200013_eng.pdf?sequence=1&isAllowed=y.

2. European Union Agency for Cybersecurity (n.d.). About ENISA (website). Available at: https://www.enisa.europa.eu/about-enisa/about-enisa-the-european-union-agency-for-cybersecurity.

3. Ibero-American Data Protection Network (n.d.). *Para el tratamiento de datos personales sobre la salud en tiempos de pandemia* [RIPD recommendations on the treatment of personal health data during a pandemic]. Available at: https:// salud-en-pandemia.pdf.

4. International Organization for Standardization (n.d.). Website. Available at: https://www.iso.org/home.html.

5. Presidency of the Nation of Argentina (2009). Law 26,529 on Patients' Rights in their Relationship with Health Professionals and Institutions. Available [in Spanish] at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/160000-164999/160432/norma.htm.

6. Government of Ecuador (2021). Organic Law 459 on Personal Data Protection. Quito: Government of Ecuador.

7. Government of Colombia (2012) Law 1,581 on Personal Data Protection. Bogota: Government of Colombia 2012. Available [in Spanish] at: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

8. Pan American Health Organization (2021). Roadmap for the Digital Transformation of the Health Sector in the Region of the Americas (resolution CD59/6). 59th Directing Council, 73rd session of the Regional Committee of WHO for the Americas. Washington, D.C.: PAHO. Available at: https://www.paho.org/en/documents/cd596-roadmap-digital-transformation-health-sector-region-americas.

9. Pan American Health Organization (2019). Plan of Action for Strengthening Information Systems for Health 2019–2023 (resolution CD57/9). 57th Directing Council, 71st session of the Regional Committee of WHO for the Americas. Washington, D.C.: PAHO. Available at: https://www.paho.org/en/documents/cd579-plan-action-strengthening-information-systems-health-2019-2023.

PAHO/EIH/IS/23-0016

PAHO Pan American Health Organization World Health Organization Americas