Privacy is health

A preliminary review of the legal framework and technological developments on electronic health records and telemedicine in Argentina

por los Derechos Civiles

Asociación por los Derechos Civiles

Supported by:

March 2021

adc.org.ar

Written by: Anastasia Dozo
Layout: Matías Chamorro
Cover design: El Maizal

1. Introduction

This paper aims to produce a preliminary general analysis of data protection regulations related to the use of information and communication technologies (ICTs) in medical care, indistinctly known as e-health or cyber-medicine.

In this sense, the intention is to provide an initial compilation of the existing norms and regulatory projects on e-health, in order to describe some of the main private and public initiatives on the subject, and to single out problems and aspects of interest that may serve as a starting point for a more in-depth study.

2. Conceptual framework

E-health is a broad and constantly evolving concept, keeping pace with the advance of technology in its application to medicine, health care as a whole, health surveillance and documentation, as well as to education, knowledge and research concerning these areas.

Within the vast field of e-health, this document will focus more specifically on electronic health records and telemedicine.

3. Legal framework

The following norms related to the processing of personal data in the field of health in the Argentinian legal system have been identified:

- The Argentinian National Constitution.
- Law 25.326 on Personal Data Protection.
- Law 26.529 on the Rights of Patients in their Relationship with Health Professionals and Institutions.
- Decree 1.558/2001 regulating Law 25.326.
- Decree 1.089/2012 regulating Law 26.529.
- City of Buenos Aires Law 5.669 on Electronic Health Records.
- Draft Bill on Electronic Health Records, Files S-1787/19, S-2849/19, 730/20, 850/20 and 1468/20.
- Telemedicine Bill Files S-538/20, S-587/20, S-627/20 AND 1405/20, consolidated into a single bill Order of the Day 205/20.
- Resolution 282/2020 of the Superintendence of Health Services.
- Provision 1/2019 of the Ministry of Health.
- Code of Ethics for the Health Care Team of the Argentinian Medical Association.

3.1. The Argentinian National Constitution

The recognition of the right to personal data protection is embodied in Article 43 of the Argentinian National Constitution, which states: "...Any person may file this action to be informed of the data referring to him or her contained in public records or data banks, or private ones intended for furnishing reports, and in case of falsehood or discrimination, to demand the suppression, amendment, confidentiality or updating of such data. The secrecy of journalistic sources shall not be affected..."

3.2. Law 25.326 on Personal Data Protection, and its Regulatory Decree 1558/2001

Law 25.326 on Personal Data Protection or "Habeas Data Law" (hereinafter, PDP Law) regulates this fundamental right to privacy and informational self-determination. According to its first article, the aim of the law is an all-encompassing protection of personal data registered in files, records, data banks or any other technical means of data processing, whether public or private, in order to guarantee the right to individual privacy and to have one's honor respected. Likewise, the law seeks to ensure access to the information recorded on them, in accordance with the provisions of the aforementioned article 43, third paragraph, of the Argentinian National Constitution.

The PDP Law and its Regulatory Decree 1558/2001 establish the legality, quality, security and proportionality for all personal information as guiding principles of data protection.

3.3. Law 26.529 on Patients' Rights in their relationship with Health care Professionals

Before expanding on the concept of Electronic Health Records (EHRs), it is necessary to mention the Medical Record (MR), which is regulated by Law 26.529 and its regulatory decree 1089/2012.

Law 26.529 defines the concept of medical record as "...the obligatory chronological, numbered and complete record in which all actions performed on a patient by health professionals and assistants are registered". Article 13 refers to digitalized medical records, establishing that they are those in which the content of the

report is delivered through magnetic media, providing they ensure the integrity, authenticity, inalterability, durability and retrievability of such data.

The MR or EHR shall contain the information that is considered essential for the truthful and updated knowledge of a patient's state of health. Its main purpose is to expedite medical assistance by listing all the information which, from a clinical point of view, allow access to this knowledge. The growing digitalization which is being experienced in all areas of life is a reality within health care institutions as well, allocating more and more resources to computerize their services and implement these new technologies.

3.4. Bill to establish a Single Federal Program for Scanning and Digitalization of Health Records within Argentina

In order to achieve an adjustment in the regulation of EHRs, there have been some normative attempts in our country, being the Bill to establish a Single Federal Program for Scanning and Digitalization of Medical Records within Argentina[1] one of particular interest. Approved by the National Senate, it pursues the consolidation of a single electronic health record for each patient. According to the bill's proponents, this unitization will offer a number of benefits: on the one hand, it will provide speed and comfort when retrieving clinical data, which in turn will save time and effort by providing access to an individual's complete medical record, regardless of the health facilities where they have been treated. On the other hand, the merge of all records into a single application will ease their reading, as it avoids the difficulties related to understanding handwritten documents.[2]

The project refers to the conditions of security, integrity, authenticity, reliability, accuracy, intelligibility, conservation, availability, access and traceability that a record must observe, as well as the updating, changes and the consultations being made to the clinical information included in the Single System of Electronic Health Records, granting recognition -at least in the letter of the text -to the guiding principles of the right to personal data protection.

However, beyond the good intentions of its authors and the mentions made in the text of the project, we should not lose sight of another aspect of this examination. First of all, the creation of a single database poses a serious risk should it not go along with adequate security measures. Considering Argentina's record in the safeguard of personal data, there are more than valid reasons to be distrustful. Information leaks or data hijackings through ransomware[3] attacks suffered by the public sector give good reasons to be wary about the vulnerability of state databases. Consequently, an attack on a future centralized information system would affect all Argentinians' sensitive health information. Secondly, the experience of our country shows that on several occasions, the gap between the letter of a law and the reality of its enforcement can be extremely broad. Beyond the principles stated in the bill, it remains to be seen whether the necessary financial and human resources are to be channeled, and to what extent there is a real understanding and readiness to preserve data security.

Furthermore, the question is whether the regulatory framework given above, together with the aforementioned bill, are suitable and sufficient to ensure that the Single Electronic Health Record System is endowed with the necessary conditions to effectively guarantee a subject's rights over their personal health data.

In this regard, the first aspect to mention is that the PDP Law distinguishes two categories of such data: a) any information referring to a natural person that determines him/her or makes him/her determinable and b) personal data specifically considered as sensitive in the Law, defining as sensitive data any knowledge related to a person's past, present or future health, either physical or mental.

Therefore, there are two types of personal information in health databases: firstly, that which identifies the person, such as first and last names, addresses, phone numbers, ID card numbers, health card numbers, etc.; and secondly, that related to the person's health record, such as diagnostic tests, surgeries, prescriptions, family history, etc., known as "medical record" (hereinafter referred to as "MR").

The EHR comprises all the documents relating to the care processes performed on each patient, with the names of doctors and other professionals involved, in order to obtain the maximum possible integration of the person's existing medical records, at least as far as each health center is concerned. The PDP Law requires the application of additional security measures to highly sensitive data, in accordance with the Patient Rights Act. Article 8 of the law allows public or private health institutions, as well as health science practitioners to collect and handle personal data related to the physical or mental health of an individual visiting or treated by them, observing the principles of professional secrecy.

Although the treatment of sensitive health information would presume the need for the data subject's explicit consent, the basis of legitimacy for its management by health care providers is established in Article 8 of the aforementioned law: the norm

indicates that consent is not mandatory as long as the processing of health data originates from a health facility in the exercise of its own functions, and providing that professional secrecy is assured.

In view of this, a doctor or a health facility is not compelled to request consent from patients for the collection and use of personal and health data if they are to be used only for the medical purposes for which they are gathered, such as diagnosis or medical treatment. However, this does not imply that such management of information has no restrictions at all. Although consent is not required, other principles of personal data protection, such as purpose, minimization, security, etc., must be complied with.

The people handling the data must be professionals subject to the obligation of secrecy, or persons under their responsibility.

This exception does not apply to all personal information collected by health care institutions, but only to health data concerning patients within the context of their medical treatment. Thus, a patient's explicit consent must be requested, for example, in the event they wish to use their data for other purposes, such as advertising.

3.5. Code of Ethics for the Health Care Team - Argentinian Medical Association

On the subject, the Argentinian Medical Association has stated, in their Code of Ethics for the Health Care Team,[4] that "a Health Record contains personal information, and there is a very personal right over it, the sole owner of which is the patient, and it should not be exposed to those who have interests other than purely professional ones on it". Specifically concerning the Electronic Health Record,

Article 185 adds that “appropriate security systems must be implemented to ensure data inalterability and prevent the action of confidential information breaching”.

Chapter 14 of the Code of Ethics regulates the use of digital technologies in health sciences, highlighting the duty to inform, the right to free, prior and informed consent, the principle of purpose and the obligation to implement effective policies and security measures which monitor the storage, access, handling or transfer of information. It establishes the obligation for people or institutions that introduce electronic health records to provide professionals with the necessary training to access the information in a suitable, timely and secure fashion, enabling the use, integrity and the highest technical quality as possible. It provides that when the use of electronic health records is applied to management, planning and research, the information stored must be related to specific needs, be anonymous or otherwise, it must procure the patient’s consent, and it must be accesed only by duly authorized persons.

3.6. City of Buenos Aires Law 5.669 on Electronic Health Records

In the Autonomous City of Buenos Aires, there is Law 5.669 on Electronic Health Records, which establishes the Integrated System of Electronic Health Records (SIHCE in Spanish) for all the inhabitants who receive health care in the Buenos Aires area, for which a single database was created, allowing the storage and management of all the health information -from birth to death- contained in electronic health records.

In line with the provisions established at a national level, in Chapter IV of Law 26,529, this act defines the Electronic Health Record (EHR) as a medical record with a unified, personal and multimedia

register fed into a database, managed by computer software and endorsed by the treating practitioner's digital signature. The regulation stipulates that the collection, updating and usage must be carried out under strict conditions of security, integrity, authenticity, reliability, accuracy, intelligibility, conservation, availability and access. The Electronic Health Record (EHR) is a computerized medical history or a digital medical record, and includes informed consents, medical and/or professional indication sheets, nursing charts, surgical protocols, dietary prescriptions, vaccination certificates, tests and practices performed, rejected or abandoned. Likewise, the Electronic Health Record (EHR) and the Electronic Health Database must include the register of a patient's willingness to donate his/her organs in accordance with and under the protection of Law 3294, the National Law on Organ and Tissue Transplants No. 24.193 and its amendment No. 26.066, as well as their status of voluntary blood donor. The medical records belong to the patient, and are confided to health facilities or supporting medical services only for handling purposes.

More specifically, in relation to personal data protection, Article 7 establishes that the Integrated System of Electronic Medical Records, the Registry of Electronic Health Records, Electronic Health Records and health information in general must comply with the principles of Accessibility, Availability, Privacy, Portability, Security, Inviolability, Confidentiality, Veracity and Authorship, Durability, Integrity, Temporality, Interoperability and standards, Finality and Timeliness.

By any means, it is worth repeating what was mentioned when referring to the bill at the national level: beyond the letter of any law, extensive research should be done on the effectiveness of its enforcement by the subjects confided to do so.

3.7. Telemedicine Bill Files S-538/20, S-587/20, S-627/20 and 1405/20, consolidated into a single bill Order of the day 205/20

As regards telemedicine, the outbreak of the Covid-19 pandemic spread its use extensively and refreshed the discussion on the norms regulating it. Social distancing measures meant that appointments between doctors and patients shifted to the virtual mode. In this context, on October 15, 2020, the Argentinian National Senate passed the Telemedicine[5] bill which, according to its text, aims to define the principles and regulate the scope of telehealth as a means of providing services and training human resources with the adoption of Information and Communication Technologies (ICTs) and devices, in order to improve health conditions and accessibility among the population, including telemedicine, tele-management, tele-education and tele-investigation.

The bill regulates the requirements and modalities of telemedicine, as well as the forms it may take, while establishing the obligation to record the medical performance in the patient's health record in accordance with the terms of Law 26,529, granting it the same validity as an in-person act. Informed medical consent is included in its legal definition, meaning the duty to inform a patient about the scope, risks, limitations and benefits of this electronic mode of clinical service and specifying the obligation to add them to his or her health record.

Article 14 establishes the conditions that must be observed in providing assistance, mentioning their compliance with the standards and conditions of service in order to ensure the mechanisms that guarantee the identification of the user and the health team members, preserving confidentiality and safeguarding the protection of personal data under the terms of Law 25.326, the rights of the patient in consonance with the provisions of Law

26.529, and the application of ethical standards and conduct of medical assistance and practices.

In this regard, it must be assessed whether the mere mention of compliance with the law on data protection in force is sufficient per se in effectively protecting the data subject's rights, or whether the telemedicine law would have to explicitly determine the measures that are necessary to ensure that the treatment of such data is duly protected. An example could be the case of tele-research, outlying the procedures and conditions under which a database that centralizes citizens' health information can be used for scientific research and development.

3.8. Provision 1/2019 of the National Directorate of Health Information Systems of the Ministry of Health and Social Development

In this sense, the Ministry of Health and Social Development Provision issued Provision 1/2019 of the National Directorate of Health Information Systems, approving the document titled *Recommendation for the use of Telemedicine,* which details the recommendations in its annex, so that the technologies used for teleconsultations ensure the quality, safety and protection of personal and sensitive data and must be subject to rigorous technical, sanitary, ethical and legal evaluations in force.

4. Current considerations

On the other hand, the different physician unions, Federación Médica Gremial, Confederación Médica de la República Argentina and the Asociación de Médicos de la Actividad Privada, have issued a joint statement[6] expressing their concern about the shift of in-person consultations to the virtual mode. It points out that private health care providers offer teleconsultation as an option of medical assistance to their members aiming to reduce operating costs and increase profits. The incorporation of technology is promoted as a way to overcome distance and thus, provide equal opportunities in health care to patients from different regions. Equally, it is argued that teleconsultation is very useful for the purpose of facilitating professional advice through electronic means. However, it cannot replace face-to-face appointments, as a doctor needs a physical examination of the patient in order to make a diagnosis.

Indeed, electronic health records and telemedicine in Argentina are a reality, being used routinely by health practitioners, health centers, social security agencies, prepaid medical insurance providers, medical product suppliers and pharmacists. Advocators of this situation claim that, as information and communication technologies advance, new applications are emerging that can be used by the health care system to improve the quality of service and broaden the concept of equality and accessibility. This would help to strengthen the continuity of the health care process based on efficiency, efficacy and effectiveness, reducing costs, streamlining actions and enabling the development of personalized medicine.

However, it is advisable to question this entirely optimistic approach. The existing situation of inequality in our country casts doubt on whether telemedicine could effectively allow low-income sectors a better access to health care. On the one hand, Internet access is relatively scarce in many regions, since it entails not only

owning a computer or smartphone, but also a quality connection in order to be able to enjoy adequate medical service. On the other hand, this reality means that many of the users of e-services are actually middle- or high-income sectors in large urban centers, hence, making telemedicine deepen rather than reduce the existing social gap.

For some years now, many health care centers have been offering services through these new media and this situation has furthered as a consequence of the COVID-19 pandemic.

Thus, on April 1, 2020, the Superintendence of Health Services issued Resolution 282/2020, which in its article 1 recommends "...that, during the term of validity of the "social, preventive and mandatory isolation" specified by Decree No. 297/20 and any extensions that may be decided, Health Insurance Agents and Prepaid Medicine Companies must implement and promote the use of tele-assistance and/or teleconsultation platforms, in order to guarantee the essential on-demand services". It then defines the concept as "...any aid and/or consultation given from distance mode, by means of adequate technologies that guarantee their delivery in timely fashion and under appropriate conditions of quality, ensuring immediate assistance within the context of a health crisis".

Regarding Personal Data Protection, Article 5 establishes the obligation for Health Insurance Agents and Prepaid Medicine Companies to guarantee that the data collected through tele-assistance and/or teleconsultation platforms and its handling respect the provisions of Law No. 25,326 on Personal Data Protection and its regulations at all times, with greater emphasis on sensitive data.

In addition, the National Ministry of Health implemented the TeleCOVID program, which allows distance communication between health professionals and patients in order to provide assistance and monitoring. The government claims that the program's strategy observes the standards of the Pan American Health Organization, according to which teleconsultations are a safe and effective way to evaluate suspected cases and guide the diagnosis and treatment of a patient, minimizing the risk of disease transmission.[7]

5. Implementations, developments and applications

The development of telemedicine in the country is not a novelty and there are organizations working on the subject for years. The following is a brief list of various actors and initiatives -both public and private- operating in the field. Similarly, a summary description of these projects, based on the statements gathered from the websites of these initiatives, will be provided.

5.1. Associations and Organizations

An example of an organization working on telehealth is the Ibero-American Telemedicine Foundation,[8] dedicated to research, development, dissemination and application of ICTs in the field of health care, which has developed the Acuario Salud System, a computerized network of Electronic Health Records for Primary Care aimed at government health and social security agencies, private medicine and pharmaceutical companies, and patients alike.

Special mention should be made of the Asociación Civil de Telemedicina de la República Argentina (Telemedicine Civil Society of Argentina - ACTRA)[9] where its members[10] have joined forces to promote the use of digital technologies in health services throughout the country.

The Argentinian Cardiology Society has also been active in promoting the use of Telemedicine, holding virtual events for the training of professionals on the subject, and forming part of the IT development, Integrando Salud de Historia Clínica Electrónica (Integrating Health and EHR).[11] Notwithstanding this, it has expressed concern about questions likely to arise, such as information security, the medical-legal aspects, professional

competence and jurisdiction issues, loss of the practitioner's privacy, working conditions and payment of medical services. It is emphasized, in general, that technology should be adopted so as to render its benefits to health care as a service for the public, not in the interest of companies.[12]

5.2. The public sector

In the public sector, we must mention the National Ministry of Health's Telehealth Coordination,[13] which aims to develop and carry out a national and federal public Telehealth policy, through the use of ICTs under standards of interoperability, security and data privacy, as a means of achieving equality in the access to medical services, reducing pressures on the public health system. This policy includes telemedicine, tele-management, tele-education and tele-research, and for its implementation, it offers the Federal Platform for Telehealth and Distance Communication and the Web Conference System for teleconsultations.

The National Network of Distance Communication Offices allows patients to access medical consultations from their places of origin, avoiding unnecessary referrals or transfers, and has more than two hundred Distance Communication Offices (DCOs) throughout the country, organized according to the different levels of tele-medical complexity. According to the program's website,[14] patients attending a local public health center and in need for a second opinion, or advice on a specialty not given in that facility, or a study requiring technology which is not available, can consult the hospitals forming part of the network in remote mode. Equally, patients being treated in high-complexity centers far from their homes can follow up on their treatment.

The Garrahan Pediatrics Hospital has implemented the Garrahan Telemedicine Program,[15] responsible for developing distance

medicine from the Hospital and became the Coordinating Center of the National Pediatric Telehealth Program in November 2016.

The program includes different forms of telehealth practices, remote medical consultations by videoconference, tele-monitoring of patients and tele-diagnosis, with an interdisciplinary team made up of doctors, administrative staff, public management graduates, institutional psychologists, social communicators, audiovisual producers and ICT management technicians.[16]

The Posadas Hospital is also part of the National Network of Distance Communication Offices in order to make its High Complexity available to all the Health Centers that comprise the country's public system. According to what is stated on its website, the aim of this Office is to formalize and institutionalize the unofficial networks with which it normally had worked and to ensure that patient referral or care is no longer an individual effort but an institutional strategy that guarantees the population access to health services. Another goal is to generate, take part in and disseminate activities carried out within the framework of the Federal Telehealth Plan, through video-conferences for training on different topics.[17]

5.3. The private sector

5.3.1. Health centers

In the private sector, many health centers have already made telemedicine available to their patients. For example, the Italian Hospital of Buenos Aires, which is a member of ACTRA, has implemented Telemedicine as a way of complementing face-to-face patient care, in cases where the use of these technologies provides the tools to meet health needs that do not require in-person

assessment. The Telemedicine program implemented includes deferred and/or scheduled teleconsultation, online spontaneous requests and tele-neuro rehab, and is based on the grounds that the exchange must take place in a safe framework, with the clinical information available to optimize results. To this end, the patient accesses the tele-consultation from his or her Personal Health Portal, whereas the practitioner does so from the patient's Electronic Health Record.[18]

5.3.2. Applications and software

Many companies also offer platforms to patients, health professionals and medical centers, which allow them to manage online appointments, patient care and reception, video consultations, billing and payment of services, medical record management, statistics, accounting administration, hospitalization, pharmacy, stock of products, and the inventory is likely to grow as new technologies applicable to the health field continue to appear.

One example is the GDC Clinic Management System,[19] which is an online software developed by Medtech which allows to handle appointments, patient care and reception, billing and settlement of services, medical record management, statistics, accounting administration, hospitalizations, pharmacy and stock, among other operational services for hospitals, clinics and other health facilities.

Saludar[20] is another digital telemedicine platform which provides teleconsultations with health professionals in different branches of medicine. Meducar,[21] in turn, offers professionals and health centers a software that enables them to manage online appointments, patient records, medical histories, secretarial services, inter-consultations, professional network and statistics. Integrando Salud[22] is a company that provides electronic medical

records and in-patient services, appointment scheduling and online appointment portal, video consultation service, patient portal, bed management, pharmacy service and billing system. Acuario Salud is another company dedicated to the development of telemedicine systems, which has created an online single electronic health record system that channels primary care and management of authorization, online audit and provision of medication through digital media.

The company Salesforce[23] also provides a system for online health care services, offering a platform which it claims to connect conversations, devices, processes, services and patient data in a safe manner. Health Cloud is a unitized digital platform for managing business processes, building relationships with suppliers and interacting with patients.

Given the spread of these services, it is necessary to put or emphasize, whatever the case is, the aspect of rights protection on the agenda. The safeguard of privacy and personal data must be an essential feature in the development of any private or public health initiative. Otherwise, the intended health inclusion – assuming it as a benefit of telemedicine, which may not be so in unequal societies such as ours- will be achieved at the cost of low-income sectors being forced to hand over their personal data in order to access essential services.

6. Preliminary conclusions

Both the Telehealth Bill and the Bill to establish the Single Federal Program for the Scanning and Digitalization of Health Records of Argentina take the data confidentiality standards established in Law 25.326 as a reference. Therefore, it is urgent and vital that all developments using Information and Communication Technologies in the field of health throughout the country fully comply with the current regulations on Personal Data Protection.

However, it must also be examined whether the creation of a Single System for the Registration of Electronic Health Records, which implies a single national database, is justified within a context where the risks of data breaches are great and the protection of information by the State is normally deficient. In this sense, part of the problem lies in the fact that the security measures necessary for the effective protection of health data have not been updated, especially if we consider that the PDP law was passed in 2000 and has become outdated after twenty years, with the passage of time and new technological developments. Likewise, the mere modernization of regulations does not guarantee their automatic compliance. It is vital to create a culture of information security and for data protection authorities to have the necessary expertise and resources to be able to supervise the observance of such standards. As long as this does not occur, it seems hazardous to propose a single database containing all the health data of the Argentinian population. The likelihood of receiving cybersecurity attacks -such as those which occurred in the databases of the National Migration Directorate or the National Road Safety Agency[24]- is considerable and the mere pledge of security does not seem to suffice in building public confidence.

Additionally, it would be interesting to consider the problems that may arise in the event that automated decisions are made

on handling health data and creating personal profiles. The General Data Protection Regulation (GDPR) and the Personal Data Protection Standards for Ibero-American States recognize a person's right not to be subject to a decision based solely on automated means, if such decision has legal consequences or if rights are affected, allowing it in case it is required to conclude or perform a contract, or if the holder has given explicit consent. On these occasions, organizations and/or companies are obliged to inform on the right to human intervention and establish the due procedures, allowing the holder to express his or her point of view and object to what is decided.

The impact assessment of activities and processes based on the use of personal information is included among the new obligations added to the European General Data Protection Regulation, and adopted by the Ibero-American Standards as well, provided that such processing may pose a risk to individual rights and freedom. The aim is to appraise the potential hazards to which personal data is exposed beforehand, and respond by adopting the necessary safeguards to reduce them to an acceptable level.

Although impact assessment is not within the obligations imposed by the current Argentinian legal system, the Argentinian Agency for Access to Public Information and the Regulatory Unit for the Control of Personal Data of Uruguay have prepared an *Impact Assessment Guide on the Protection of Personal Data,*[25] not legally binding and for guidance, which follow this new international recommendation.

For medical research, the development of policies in public health and epidemiology, and the elaboration of statistics, a unified database including all health information can be an extremely valuable asset. However, it is necessary to establish the anonymization of the database as a requirement, in order

to mitigate the risks presented by the massive collection and processing of personal data. A process which encrypts sensitive information should be incorporated, so that the rights of data subjects are not infringed.

The risks and levels of impact of non-compliance with legal provisions and security measures is high, so it is vital to devise a scheme for the implementation of controls to prevent potential security incidents, unauthorized access and data breaches, as these can cause serious harm to data subjects. It is likely that a future debate on new regulations on this matter will be the best opportunity to include measures that raise the standards of compliance with international guidelines on data protection and consider references such as the Personal Data Protection Standards for Ibero-American States or the General Data Protection Regulation -without this meaning that such standards cannot be criticized or evaluated for improvement- in order to guarantee the protection of citizens' rights.

7. Notes

1 https://www.senado.gob.ar/parlamentario/parlamentaria/387980/downloadPdf

2 https://www.infobae.com/salud/2020/11/30/de-que-se-trata-el-proyecto-de-ley-de-digitalizacion-de-historias-clinicas-que-obtuvo-media-sancion-de-senadores/

3 Ransomware is a malicious software program that infects your computer and displays messages demanding the payment of money to restore the system's operation: https://www.kaspersky.com/resource-center/threats/ransomware

4 https://www.ama-med.org.ar/page/Codigo_de_Etica-2da_Edicion

5 https://www.senado.gob.ar/parlamentario/parlamentaria/ordenDelDiaResultadoLink/2020/205

6 http://asociacionamap.org.ar/upload/PROYECTO%20DE%20LEY%20DE%20SALUD%20DIGITAL%20(3).pdf

7 https://www.argentina.gob.ar/salud/coronavirus/telecovid

8 Fundación Iberoamericana de Telemedicina: http://telemed.org.ar/

9 http://actra.com.ar/

10 Acudir, ASE, CEMIC, Emergencias, Fleni, Halitus, Oroño Group, German Hospital, British Hospital, Italian Hospital, Private Community Hospital, Private University Hospital of Córdoba, Austral University Hospital, Cardiovascular Institute of Buenos Aires, Leben Salud, Omint Group,

OSDE, Rossi Center, Sanatorio Mater Dei, SanCor Salud, Sanity Care, Siempre, Stamboulian, Swiss Medical Group, URG Urgencias, Vital, YPF Obra Social and Zaldívar Institute.

11 https://www.sac.org.ar/historia-clinica-electronica/

12 https://www.sac.org.ar/consejos-cientificos/en-tiempos-de-telemedicina-reflexiones-sobre-la-atencion-medica-virtual/

13 https://www.argentina.gob.ar/salud/telesalud/definicion

14 https://www.tistudios.com.ar/garrahan/web/v3/telemedicina.html

15 https://www.garrahan.gov.ar/telemedicina

16 https://www.tistudios.com.ar/garrahan/web/v3/equipoTelemedicina.html

17 https://www.argentina.gob.ar/salud/hospital-nacional-posadas/profesionales/oficina-de-comunicacion-distancia

18 https://www1.hospitalitaliano.org.ar/#!/home/telepacientes/inicio

19 https://www.clinicas.com.ar/landingpagesgdc/lp-gdc/lp-gdc.asp

20 https://saludar.com/

21 https://www.meducar.com/

22 https://www.integrandosalud.com/es-ar/

23 https://www.salesforce.com/solutions/industries/healthcare/health-cloud/

24 ADC, “10 noticias relevantes para la privacidad en Argentina” [10 relevant news for privacy in Argentina], March 2021: https://adc.org.ar/2021/03/11/10-noticias-relevantes-para-la-privacidad-en-argentina/

25 https://www.argentina.gob.ar/sites/default/files/guia_final.pdf

adc.org.ar