Perspectivas LEGA

Caracas, April 23, 2025

N° PL0028

ELECTRONIC MEDICAL RECORDS AND PROTECTION OF PERSONAL DATA OF PATIENTS

Rosa Virginia Superlano
Partner

The protection of personal data is an issue of growing importance and its management in the health sector does not escape that relevance, especially in a context where the digitization of medical information has accelerated. In Venezuela, although there is no special law on the protection of personal data, the Constitution and other regulations establish a regulatory framework that seeks to guarantee the privacy and security of patient information.

Articles 28 and 60 of the Constitution provide for the protection of the honour, private life and intimacy of individuals and their personal data. These constitutional guarantees have been interpreted by the Constitutional Chamber of the Supreme Court of Justice, in judgment No. 1318 of August 4, 2011, which established minimum protection criteria that must be complied with when handling personal data of third parties, including health information.

Medical information is considered one of the most sensitive types of data, and its unauthorized disclosure can have serious consequences for the privacy and dignity of patients and even their families. Therefore, this protection is especially relevant in the face of the practice – more frequent by day – of the use of telemedicine and the adoption of Electronic Medical Records (EMRs) that increase the amount of personal data that is handled digitally, which poses significant challenges to the compilers and administrators of these systems to guarantee their security and confidentiality.

I. The EMRs

There is no doubt that the use of EMRs or *Electronic Health Records* (EHRs) – which are electronic files with information on a patient's complete medical history – represent a powerful tool that brings great benefits to the patient, health professionals and public and private hospital institutions. They allow for quick

access to patients' medical information, facilitating more accurate diagnoses and more effective treatments, reducing the possibility of errors and misinterpretation of data, and warning of other existing ailments, such as drug interactions, allergies, and other health conditions, thus improving patient safety and optimizing patient treatment.

EMRs facilitate coordination between health providers, providing a smoother and more immediate exchange of information and more comprehensive health care. They also optimize the use of both material and human resources in the provision of health services. They also allow the integration of data, which is leading to the creation of national and even regional electronic health systems in many countries.

EMRs can also incorporate family, sociological, educational, and economic data. Naturally, they compile and generate a large amount of medical data on patients, information that is considered highly sensitive. In addition to the benefits already described, they are useful for medical research and health policymaking, which can help identify trends, evaluate the effectiveness of treatments, and improve resource planning. This makes that data highly coveted and susceptible to cyberattacks and unauthorized access.

II. Obligation to protect patients' personal data

EMRs are not exempt from guaranteeing the confidentiality of patients' personal data and must comply with the minimum protection requirements: patient consent, information on the purpose to be given to the data offered and authorisation for this purpose, possibility of revocation of authorisation, proportionality and guarantee of confidentiality. Its use should be limited to health professionals.

Due to current trends, the implementation of EMRs is leading to the use of the substitution of traditional printed "medical records", which in Venezuela the Organic Health Law enshrines as a right of the patient. This Law states that they must contain, in writing and certified by the treating physician, all the data pertinent to their disease, reason for consultation, history, history of the current disease, main diagnosis and secondary diagnoses, therapeutic and clinical evolution. Likewise, this Law enshrines as a right of the patient the confidential treatment of medical information about his person. Currently, there is no special rule that regulates medical records in detail.

However, the Code of Medical Deontology provides ethical guidelines for the preparation and management of medical records, indicating that physicians must record complete, accurate and updated information on the patient's state of health, access reserved to medical professionals with the obligation of confidentiality, and may be shared only with the patient's consent or by legal mandate.

It should be taken into account that it is increasingly common for medical records or medical records to be contained in RMH systems, therefore, the provisions on data protection coincide with the special rules that regulate digital media in Venezuela, the Law on Data Messages and Electronic Signatures and the Special Law against Computer Crimes.

These laws are essential to facilitate the safe and legal use of electronic health systems in Venezuela; ensuring that EMRs have legal validity, and protecting patients' medical information, also include security measures to prevent misuse and sanction the violation of electronic systems.

III. Responsibility

It should be taken into account that the improper disclosure of patients' personal data can lead to serious legal consequences for health professionals and medical institutions that have the responsibility of ensuring the confidentiality of the medical information poured into the systems.

This liability arises not only from disclosing patient information to unauthorized third parties (exceptions allowed by law are excluded here), but also from its unethical handling and consenting to improper access to it due to careless or negligent handling of RMH.

The Special Law against Computer Crimes protects the confidentiality, integrity and availability of the data stored in the EMRs and classifies as crimes various behaviors that can affect them, such as unauthorized access, data manipulation and computer sabotage. Penalties can include fines and imprisonment; consequently, health professionals and institutions that handle EMRs may be criminally liable if they do not adequately protect EMRs and the information contained therein.

IV. Challenges

Perspectivas LEĜA

For the use of EMRs to be optimal, reliable management must be guaranteed with accurate, complete and updated patient information, poured into compatible, robust and new generation technology environments.

At the same time, it is a challenge for public and private health professionals and institutions, which must adopt good practices and robust security measures to guarantee the privacy and protection of patients' personal data. They should also be zealous in procuring appropriate EMR providers and programmes; This includes the use of encryption systems, *firewalls* and cybersecurity protocols and rigorous and specialized training for personnel who handle these systems.

Thus, the proper implementation of these regulations is crucial to ensure trust and security in the use of digital technologies in the health sector and the protection of patients' medical information, remembering that the privacy of personal medical data is an obligation for health professionals and the compilers and administrators of these databases. and a right of patients that must be guaranteed.

Contacts:

Rosa Virginia Superlano
E-mail: rsuperlano@lega.law
Phone: +58 (0212) 2772236

LEĜA Abogados
Office:
+58 (212) 277.22.00
E-mail: infolaw@lega.law
Web: www.lega.law