ISSN: 2230-9926

Available online at http://www.journalijdr.com

IJDR

International Journal of Development Research
Vol. 10, Issue, 10, pp. 41188-41192, October, 2020
https://doi.org/10.37118/ijdr.20282.10.2020

RESEARCH ARTICLE OPEN ACCESS

THE GENERAL DATA PROTECTION LAW IN HEALTH

***Soraya Pereira and Dr. Ycarim Melgaço Barbosa**

Department Territorial Planning and Development, Pontifical Catholic University of Goiás - PUC, Goiânia, Brazil

ARTICLE INFO

Article History:
Received 11th July, 2020
Received in revised form
28th August, 2020
Accepted 04th September, 2020
Published online 24th October, 2020

Key Words:
Data storage; Personal data;
Safety; Health units.

****Corresponding author: Soraya Pereira,***

ABSTRACT

This article addresses the General Data Protection Law (LGPD) and its applicability in health, to ensure the security and privacy of the patient's personal data, generated in the health unit. **Objective**: to seek to identify the security mechanism adopted by the health organization for the storage and treatment of patient data, informed during the provision of medical and hospital services. **Method**: it is understood that a qualitative analysis of bibliographic information, study of legislation and scientific publications on the Internet is essential, with methods and forms of approach that guarantee the consistency of the study, which was supported by authors who conceptualize, approach and analyze the LGPD highlighted in the hospital field, a situation in which you must freely and spontaneously consent to the use of your personal information. **Results**: to guarantee the confidentiality of information, it is essential to protect and process data, in a safe and transparent manner, in compliance with the relevant legislation. **Conclusion**: it was found that the assurance of information security and the encryption of databases is essential to prevent the health unit from breaching the LGPD and incurring severe penalties provided for therein.

Citation: ***Soraya Pereira and Dr. Ycarim Melgaço Barbosa, 2020.*** "The general data protection law in health*", International Journal of Development Research*, 10, (10), 41188-41192.

INTRODUCTION

In the digital world, which presents instant facilities created by technology, users provide their personal data to third parties, in countless Internet sites and applications, products or services, without questioning and without any security regarding the misuse of their information, which can be made available without their consent and misused, which can lead to leakage of data and cybercrime, causing damage to individuals, legal entities and the State itself. In order to curb the misuse of personal information and avoid damages to the image of individuals, legal entities and the State itself, came the inspiration for the enactment of the first Brazilian legislation to protect personal data, known as LGPD, in 2018, using as a model the General Data Protection Regulation of the European Union (GDPR), aiming to fill a gap to ensure the privacy of information of Brazilian citizens, as guaranteed by fundamental rights (Cots & Oliveira, 2019, p. 7). This article analyses the Law no. 13.709, of August 14, 2018, known as the General Data Protection Law (LGPD), and its applicability in the health field, to guarantee the security to protect the privacy and personal data of natural persons, originated from the information provided by the patient, which compose your medical record, during the medical-hospital care, in person or via telemedicine, at the health unit. In order to carry out the research, it is sought to identify the processes adopted by the health unit for storage and treatment of patient data, considered sensitive by LGPD, informed during the provision of medical-hospital services, in outpatient or inpatient care, in particular, agreements or insurance companies, aiming at the excellence of services offered and the safety of the patient. In view of the above, the following question arises: what is the security mechanism adopted by the health unit for the storage and treatment of patient data, informed during the provision of medical-hospital services, in outpatient or inpatient care, in particular, agreements or insurance companies, to ensure the privacy of personal data and sensitive data, provided and components of their records?

The treatment of personal data by the health unit must be based on a consistent system of information technology, strictly obeying the legal grounds for the treatment of personal data, to provide legal security, objectively and clearly, to protect the privacy of patients. It is understood that a qualitative and quantitative analysis of bibliographic information, including research in books, newspapers, magazines, reports, legislation, official documents of public

interest and on the Internet, with methods and forms of approach that ensure the consistency of the study, is indispensable. The theoretical basis of this study was based on authors who approach and analyze LGPD, which represents the legal framework in data protection in Brazil, with emphasis on the hospital field, a situation in which individuals provide their personal data at the time of a medical-hospital care. The contributions of authors such as Cots and Oliveira (2019), Bessa (2019), Maldonado and Blum (2019), Brancher and Beppu (2019) and Bioni (2020), which bring to light relevant issues regarding data ownership, privacy, consent and protection of personal data, is therefore essential. These issues are of paramount importance in the approach to be taken.

Overview and Hypothetical use of Patient Data: Patient S.P., resident in another state, schedules a medical-hospital service, via an internet application, fills out the registration form provided by the health unit, informing his/her personal data, including date and time and all pertinent information. From the sending of these data, S.P. accesses a website for the sale of air tickets, which for your surprise, sends information about lodgings, restaurants, car rental companies, clinics and laboratories to perform diagnostic tests, among others. In view of the above, what for S.P. looked like the facilities provided by the use of technology, for its stay during its supposed care in a health unit in another location, becomes a great torment, given the exponential sharing of your personal data, with numerous product and service companies, exposing your data without any security, including for improper use, indiscriminate, without your consent and control, causing damage to your image and causing financial losses, by fraud committed in your name.

The security and privacy of patients' personal data before LGPD: In the legal framework, before the LGPD, the treatment of data and fundamental rights were arranged in the 1988 Federal Constitution, in its article 5, item X, which brings the guarantee of privacy and inviolability:

> Article 5 - Everyone is equal before the law, without distinction of any nature, guaranteeing Brazilians and foreigners residing in the country the inviolability of the right to life, freedom, equality, security and property, under the following terms: (...)
> X - the intimacy, private life, honor and image of people are inviolable, ensuring the right to compensation for material or moral damage resulting from their violation (Constitution of the Federative Republic of Brazil, 1988, n. p.).

In the same vein, Law No. 8.078/1990: Consumer Protection Code, in its Article 43, established the creation of consumer databases; Law No. 10.406/2002: Civil Code disciplined in its articles 11, 12, 16 and 17, the rights relating to privacy and intimacy; in Resolution CFM No. 1.821/2007, in its Article 2, provides on the protection of medical data and electronic record:

> Article 2 - Authorize the digitization of patients' records, provided that the mode of storage of the digitized documents complies with the specific norm of digitization contained in the paragraphs below and, after mandatory analysis by the Review Commission of records, the rules of the Permanent Commission for the Evaluation of Documents of the medical-hospital unit that generates the archive.
> §1 Scanning methods must reproduce all the information of the original documents.
> §2 The digital files originated from the digitalization of the documents in the patient's records must be controlled by a specialized system (Electronic Document Management - EDM), which has, at least, the following characteristics:
> a) Ability to use appropriate database for the storage of digitized files;
> b) Indexing method that allows to create an organized archiving, allowing the search in a simple and efficient way;
> c) Compliance with the requirements of "Security Assurance Level 2 (NGS2)", established in the Manual for Certification of Electronic Health Record Systems (Cots & Oliveira, 2019, p. 33).

The importance of LGPD for the health unit : In order to avoid leakage and misuse of personal data, specifically in the case at hand, in the Health Sector, LGPD was created to give a new legal security guise to consumers, who are the patients and to the Health Units and their professionals, who contract services among themselves and with third parties, such as: image, laboratory and diagnostic exam services, guaranteeing protection to the data generated during the provision of medical-hospital services. According to Brancher and Beppu (2019, p. 88), "personal data is all information related to the identified or identifiable natural person", such as the information contained in documents that identify a natural person, in the case of CPF, Identity Card, full name, affiliation, among others. To facilitate understanding, we will make a comparative table, according to the provisions of Article 5 of the LGPD (Law No. 13.709, 2018), which brings the definitions of personal data, sensitive personal data, anonymized data and database:

Table 1. Definitions provided in Article 5, Items I, II, III and IV of the LGPD

PERSONAL DATA	SENSITIVE PERSONAL DATA	ANONYMIZED DATA	DATABASE
I - information related to identified or identifiable natural person.	II - personal data on racial or ethnic origin, religious conviction, political opinion, union membership or religious, philosophical or political organization, data concerning health or sexual life, genetic or biometric data when linked to a natural person.	III - data relating to a data subject who cannot be identified, considering the use of reasonable and available technical means at the time of their processing.	IV - structured set of personal data, established in one or several locations, in electronic or physical support.

Source: (Law no. 13,709, 2018).

In the health unit personal data and sensitive data of the patient will be used, which will be part of the medical record, the request and results of laboratory tests, image and diagnosis, for elucidation of the diagnostic hypothesis, which will be part of the database, which should be organized, coordinated, fed, controlled and excluded, according to the request of the data subject, by the information technology sector, obeying the strict criteria of data privacy security and

pertinent legislation. In this sense, the professionals who work in the Health Units will have their responsibility extended in order to guarantee the confidentiality of the information, as well as the security of the treatment of sensitive data of patients and of other professionals involved in the rendering of the medical-hospital services offered to the population, in the health units, public and private, obeying the norms established by the inspection and regulatory agencies, such as the National Agency of Supplementary Health (ANS) and the Class Councils.

Patient's consent: Article 7, item I, and Article 8 of the LGPD provide that the consent of the data subject, as provided in Article 104, items I, II and III of the Civil Code: "I - capable agent; II - lawful, possible, determined or determinable object; and III - form prescribed or not defended by law" (Law No. 10.406, 2002, n.p.) shall be provided by free and spontaneous will, preferably in writing, with the purposes specifically determined and with a clause detached from the others, in order to avoid consent addiction, being that the burden of proof falls on the controller (Cots & Oliveira, 2019, pp. 90-92). Without the consent of the data subject, as provided for in Article 11, Subsection II, of the LGPD, in those cases where it is indispensable to do so: "e) protection of the life or physical safety of the subject or third party; f) protection of health, in procedures performed by health professionals or health entities" (Brancher & Beppu, 2019, p. 41). The patient may revoke his/her consent at any time, by his/her express manifestation, not necessarily in writing, in an easy and free way. From this revocation, consequences arise to be observed: "that the treatment carried out before the revocation is maintained until there is a request for elimination of personal data" (Cots & Oliveira, 2019, p. 96). The same means that consent was collected must be observed in order to allow its revocation. If it was through the internet, it must be done through the internet.

Treatment of the patient's personal data: The personal data of the patient, regardless of the method (analog or digital) and the relationship with the data subject, who is a "natural person to whom the personal data that are the object of treatment refer" (Brancher & Beppu, 2019, p. 87).

context, we will use the sensitive data. According to Brancher and Beppu (2019, p. 88), the treatment "is every operation performed with personal data", with a broad concept that involves "everything that can be done with personal data, from the collection to the disposal of this information". LGPD specifies not only the collection of data, but also, access, use, classification, reception, processing, storage, transfer, elimination, modification, among others.

Personal data processing agents: The treatment agents are the operator and the controller. According to Brancher and Beppu (2019, pp. 88-89): "The controller is the natural or legal person, under public or private law, who is responsible for decisions regarding the processing of personal data. In the case of patient data, it is the hospital unit that controls and determines the way the data should be processed and chooses the operator to comply with the decision taken and comply with the instructions previously defined. The person in charge "is the natural person, indicated by the controller to act as a communication channel between the controller, the data subject and the National Data Protection Authority" (Brancher & Beppu, 2019, p. 89). The law requires publicity and disclosure of the data that identify the controller, as well as the disclosure of his contact, on the controller's website, in a clear and transparent manner. Among the functions of the controller, according to LGPD, is the resolution of complaints coming from the data subject, taking the appropriate measures, adopting measures in attendance to the National Authority, informing and guiding employees and contractors, about the personal data protection system, regardless of the person in charge, being an employee of the controller or residing in Brazil, as long as it acts as a communication channel between those involved, National Authority, data subject and represents the controller (Brancher & Beppu, 2019, p. 89). According to the provisions of Article 5 of the LGPD (Law No. 13,709, 2018), the definitions of data subject, controller, operator and person in charge are as follows:

Regarding good practices and governance, described in Section II of the LGPD, specifically in article 50, which provides on the competence of controllers and operators to establish the internal supervision and control mechanisms, the

Table 2. Definitions provided in Article 5, Items V, VI, VII and VIII of the LGPD

DATA SUBJECT	CONTROLLER	OPERATOR	OVERSEER
V - natural person to whom the personal data that are the object of treatment refer; In our study, this is the patient.	VI - natural or legal person, of public or private law, to whom the decisions regarding the treatment of personal data compete; In our study, it is the health unit, public or private.	VII - natural or legal person, of public or private law, who performs the treatment of personal data on behalf of the controller; In our study, it is the sector of information technology of the health unit.	VIII - person indicated by the controller and operator to act as a communication channel between the controller, the data subject and the National Data Protection Authority (ANPD); In our study, this is a person indicated by the senior management of the health unit.

Source: (Law no. 13,709, 2018).

As of the LGPD's validity, in article 11, which states: "The treatment of sensitive personal data" and cites the hypotheses in which it must occur, from the moment a patient enters a Health Unit, he or she must, obligatorily, himself/herself same or his or her legal responsible, consent in a free, clarified, specific and detached way, the right of the use of his or her personal data, obeying the rules of professional secrecy, keeping and handling of the patient's file, in observance of the legal previsions (Cots & Oliveira, 2019, p. 107). In order to process patient data, it is necessary to separate personal data, identified or identifiable, sensitive data and anonymized data, regardless of whether they are online or offline, which in this

actors responsible for the implementation of safety procedures, educational actions in the organizational environment, aiming at minimizing risks in the treatment of personal data, the health unit shall promote the solution of petitions and complaints from data subjects, individually or through outsourcing, aiming at resolving conflicts and reestablishing the patient's trust in the medical-hospital services provided by the health unit (Law No. 13.709, 2018, n.p.).

Rights of the patient data subject: According to Cots and Oliveira (2019, p. 126), as stated in Article 17 of the LGPD: "Every natural person is assured the ownership of his personal data and guaranteed the fundamental rights of freedom,

intimacy and privacy, in accordance with this Law". Therefore, the patient has the right to withdraw his personal data, since the rights of his personality are non-waiverable and non-transferable.

LGPD brings in several articles, the rights granted to the data subject:

- ownership of personal data;
- rights in relation to the controller;
- right of confirmation of processing;
- right of access;
- correction of incomplete, inaccurate or outdated data;
- anonymization, blocking or deletion of data;
- portability of data to another supplier of products or services;
- deletion of personal data processed with the consent of the data subject;
- shared use of data;
- possibility of not providing consent;
- revocation of consent;
- right of petition; and
- right of opposition (Brancher & Beppu, 2019, pp. 90-97).

In the situation where the data subject is a patient, he can access his data in the health unit, for corrections of eventual failures, portability for use in other hospitals, clinics, laboratories and companies providing services or selling products, including asking for the exclusion of the controller's database, in order to have ownership of them. And, if you need to file an extrajudicial or judicial claim, you are entitled to your right and petition.

Governance, IT, compliance and legal: In order to implement LGPD, obeying all the criteria required by it, governance must adopt internal management policies, restructuring the health unit, seeking an action plan to promote the necessary changes to comply with the referred law, as well as readapt processes and people, starting with employee training, specifically regarding the personal data of all those involved in the medical-hospital care provided to the patient, with the implementation of technical measures for protection and security to the treatment of personal data and sensitive data of the patient. Seeking the implementation of action policies, it is necessary to align the management teams, highlighting the importance of information technology to choose a program that translates security, privacy, efficiency and effectiveness in the treatment of information, with the encryption of the database of patients, as well as the assurance of compliance and the integrity program, known as compliance, allied to legal advice, aiming to prevent any non-compliance, especially with regard to the consent form, in compliance with the LGPD, to inspire confidence to the users of the health unit, avoiding incurring administrative sanctions and the payment of fines.

National Data Protection Authority (ANPD)

The ANPD, according to the provisions of article 52, clauses I and II, of the LGPD, may charge the infringing agent with the following penalties:

I - warning, with indication of deadline for adoption of corrective measures;
II - a simple fine of up to 2% (two percent) of the turnover of the private legal entity, group or conglomerate in Brazil, in its last fiscal year, excluding taxes, limited in total to R$ 50,000,000.00 (fifty million reais) per infraction;
III - daily fine, observing the total limit referred to in clause II;
V - publication of the infraction after duly ascertained and confirmed its occurrence;
V - blocking of the personal data referred to in the infraction until its regularization (Law no. 13.709, 2018, n. p.).

The National Data Protection Authority (ANPD) was created by Provisional Measure No. 869/2018, and is the public administration body responsible for overseeing, implementing and inspecting compliance with LGPD. The ANPD, according to article 51 of the LGPD (Law no. 13.709, 2018, n. p.), provides: "the national authority shall encourage the adoption of technical standards that facilitate the control by the data subject of their personal data", and has the following composition: Board of Directors, National Council for Personal Data Protection and Privacy, civil society, representatives of the Public Power, ombudsperson's office, tax authorities, business sector and ombudsperson's office, administrative and specialized units, and its own legal advisory body, to deliberate and interpret the Law, edit personal data protection rules and inspect and apply penalties to offenders (Brancher & Beppu, 2019, pp. 89-90).

RESULTS

To guarantee the secrecy of the information, from the scheduling of the first appointment, via telephone or internet, to the appointment, in person or via telemedicine, became indispensable to the implantation and adaptations in the processes, training of people and tools in the use of a robust system of treatment and storage of the data, by means of the information technology, considering the use of artificial intelligence and disruptive innovation, implementing policies to protect the privacy and security of the data informed by the patient, as well as the data contained in his or her medical records, which are kept in a physical or electronic file, in compliance with the provisions of the LGPD and the legislation in force. It is not intended to exhaust the subject in this study, but it remains clear that LGPD has come to curb misuse and prohibit the sharing of personal information of patients and others involved in medical-hospital care processes, with the implementation of technical standards to facilitate access and control by the data subject of personal data, the definition of specific functions for those responsible for the collection, storage, use, deletion and treatment of data, as well as the resolution of complaints presented by patients and the inspection by the national authority, in order to avoid damages to individuals, companies and the State, such as the practice of selling data between companies of products and services and crimes, by physical or digital means, with the inspection and application of severe administrative penalties and fines to offenders, given the globalization, technological evolution and exponential transmission of information sharing.

Final Considerations

During the study, specifically the application of LGPD in health, it was verified, through analysis, that the Law came to guarantee the protection of the fundamental rights of the Brazilian citizen, essentially with the assurance of the security of the information provided by the patient and other

professionals involved in the provision of medical-hospital services, with the cryptography of the databases, to avoid damages to the image of the people and to restrain severe penalties to the health units and their legal representatives.

LGPD has 65 articles and was inspired by the GDPR, used in the European Union, and came to curb the misuse of personal information and avoid damage to the image of individuals, legal entities and the State itself, due to the violations committed, such as the practice of cybercrimes, with the application of severe administrative sanctions and fines, applied by the national authority, ranging from 2% (two percent) on the revenues of the legal entity, private law, or group of companies, in Brazil, after the exclusion of taxes and limited to the amount of R$ 50,000,000.00 (fifty million reais) per infraction committed by a health unit. From this perspective, in order to avoid the administrative sanctions foreseen in LGPD, the senior management of the health unit establishes safety standards for the information of the data subject, professionals and other actors involved and participants in the multiprofessional patient care teams, maintaining the assurance of compliance and integrity program, known as compliance, required by the competent inspection agencies and strictly obeying the criteria established in LGPD and other pertinent legislations for the security of privacy and intimacy of individuals, offering medical-hospital services of excellence, guaranteeing a prominent place in the market, promoting the technological, economic and regional development of the Brazilian health sector.

REFERENCES

Bessa, L. R. 2019. *Nova Lei de Cadastro Positivo: comentários à Lei 12.414, com as alterações da Lei Complementar n. 166/2019 e de acordo com a LGPD*. São Paulo: Thomson Reuters Brasil.

Bioni, B. R. (2020). *Proteção de dados pessoais: a função e os limites do consentimento* (2a ed.). Rio de Janeiro: Forense.

Brancher, P. M. R. & Beppu, A. C. (2019). *Proteção de dados pessoais no Brasil: uma nova visão a partir da Lei nº 13.709/2018*. Belo Horizonte: Fórum.

Constituição da República Federativa do Brasil de 1988. (1988). Recuperado em 10 de setembro, 2020, de https://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm

Cots, M. & Oliveira, R. (2019). *Lei geral de proteção de dados pessoais comentada* (3a ed.). São Paulo: Thomson Reuters Brasil.

Lei n.º 10.406, 10 de janeiro de 2002. (2002). Institui o Código Civil. Recuperado de http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm

Lei n.º 13.709, 14 de agosto de 2018. (2018). Lei Geral de Proteção de Dados Pessoais (LGPD). Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Lei n.º 8.078, 11 de setembro de 1990. (1990). Dispõe sobre a proteção do consumidor e dá outras providências. Recuperado de http://www.planalto.gov.br/ccivil_03/leis/l8078.htm

Maldonado, V. N. & Blum, R. O. (2019). *Comentários ao GDPR* (2a ed.). São Paulo: Thomson Reuters Brasil.

****