ARQUIVOS DE ASMA, ALERGIA E IMUNOLOGIA

Special Article

Starting an Allergy and Immunology practice. Part 3 – GDPR for doctors: Basic concepts and responsibilities

Construindo o consultório do Alergista e Imunologista. Parte 3 – LGPD para médicos: conceitos básicos e responsabilidades

Eduardo Magalhães de Souza Lima[1], Adriana Aragão Craveiro Leite[2], Celso Taques Saldanha[2], Fátima Rodrigues Fernandes[2], Gustavo Falbo Wandalsen[2], Luís Felipe Chiaverini Ensina[2], Fábio Chigres Kuschnir[3], Dirceu Solé[4], Henrique Cunha Lima[5], Fernanda Amaral Duarte[6], Lorenzzo Anonini Itabaiana[7]

ABSTRACT

The Brazilian General Data Protection Regulation (GDPR) regulates the processing of personal data, establishing specific rules for its protection. Medical practices must comply with the GDPR as well as with the Medical Ethics Code, as they handle sensitive health-related data. Noncompliance can result in severe administrative and legal penalties. To ensure compliance, it is crucial to implement a Data Protection and Governance Program, which includes security measures and the documentation of data processing activities. In addition, obtaining liability insurance, particularly cyber insurance, is recommended as a way of mitigating the risks that doctors naturally face when conducting their activities.

Keywords: Computer security, data protection, information protection, liability, insurance.

RESUMO

A Lei Geral de Proteção de Dados (LGPD) regulamenta o tratamento de dados pessoais, impondo regras específicas sobre sua proteção. Clínicas médicas devem cumprir a LGPD além do Código de Ética Médica, pois lidam com dados sensíveis, como informações de saúde. O não cumprimento dessa Lei pode resultar em penalidades administrativas e judiciais severas. Para conformidade, é crucial implementar um Programa de Governança em Proteção de Dados, que inclui medidas de segurança e registro de operações de tratamento. Recomenda-se, ainda, a contratação de seguros de responsabilidade, em especial seguros cibernéticos, como forma de mitigar os riscos que os médicos naturalmente incorrem no desenvolvimento de suas atividades.

Descritores: Segurança computacional, proteção de dados, proteção da informação, responsabilidade, seguro.

Introduction

You run a private medical practice and handle personal data from several patients every day. These data are essential for providing care and often contain sensitive information about patients' health conditions.

In 2018, a law was passed in Brazil to regulate the processing of personal data across all sectors of the economy: the Brazilian General Data Protection Regulation (GDPR).[1] Although enacted in 2018, the

1. Coordinator of the Statute, Regulations, and Standards Committee of the Brazilian Association of Allergy and Immunology (ASBAI) – 2023/2024 Term.
2. Member of the Statute, Regulations, and Standards Committee of ASBAI – 2023/2024 Term.
3. President of ASBAI – 2023-2024 Term.
4. Research Director at ASBAI – 2023-2024 Term.
5. Attorney, Master of Digital Law from the Universidade Federal de Minas Gerais (UFMG). Professor of Data Protection and Digital Law at the Pontifícia Universidade Católica de Minas Gerais (PUC Minas) and CEDIN.
6. Attorney, Master of Laws from the UFMG. IT Technician specialized in computer programming – CEFET-MG.
7. Attorney, Master's Student of Law and Technology at UFMG, Postgraduate in Digital Law from PUC Minas.

Submitted Apr 21 2024, accepted Nov 02 2024.

Arq Asma Alerg Imunol. 2024;8(4):362-70.

http://dx.doi.org/10.5935/2526-5393.20240049-en

GDPR only came into full effect in August 2021. During the nearly 4-year transition period, the imposition of administrative sanctions was suspended, giving data controllers time to comply with the new requirements and allowing the establishment of the Brazilian Data Protection Authority (Autoridade Nacional de Proteção de Dados, ANPD) – the agency responsible for enforcing the law. Since then, the ANPD has received numerous complaints, launched administrative and sanctioning proceedings, and even issued its first fine for noncompliance with the GDPR in 2023.

The Brazilian GDPR outlines how personal data must be handled and intersects with other regulations, such as the Medical Code of Ethics. For this reason, it should be studied by everyone who handles personal data, regardless of the volume of data or the size of the medical practice.

This article will address the main precautions that must be taken when handling patient data, including an overview of key GDPR concepts and the context of digitalization in health care services. It will also describe the legal responsibilities – both administrative and civil –physicians may assume in the course of data processing.

Basic concepts

What is personal data?

Personal data are any information relating to an identified or identifiable natural person. In other words, personal data must relate to a physical individual and either directly identify them or have the potential to do so. An example of the first case is the CPF (Taxpayer Identification Number), which directly identifies its holder. In the second case, it is necessary to consider whether a combination of information can identify someone. For example, in a game of Secret Santa, as more characteristics of a person are revealed, they become increasingly identifiable. This means that even seemingly trivial information, such as hair color, height, or clothing, can identify someone depending on the context.

Therefore, a person's health information may also lead to their identification, whether because they have a rare disease or because they are a public figure whose health condition is widely known.

The Brazilian GDPR also defines a specific category of personal data that requires a higher level of protection: sensitive personal data. These are data that could lead to discrimination against the individual, such as those related to racial or ethnic origin, religious beliefs, political opinions, or health data. Such data may only be processed under restricted circumstances, requiring additional precautions. For example, these data cannot be shared for commercial advantage, unless the sharing is strictly necessary for the provision of services. A hospital, for instance, may share health data with health insurance providers, but may not sell them to a pharmaceutical company.

Important note: Many people mistakenly believe that data such as CPF numbers, balance sheets, and bank statements are classified as sensitive personal data. This is not the case. While such information is indeed important and must be protected, it is not defined as sensitive under the Brazilian GDPR. Understanding this distinction is crucial for identifying the appropriate legal basis for processing different types of data – which will vary depending on whether the data are regular or sensitive. Do not worry if you are not familiar with the term "legal basis." We will cover what it is and why it matters in the following sections.

Processing of personal data

The Brazilian GDPR applies to all activities that fall under what it defines as "processing of personal data." Therefore, in addition to understanding what qualifies as personal data, it is also essential to understand the concept of data processing. The GDPR outlines a broad range of actions that constitute data processing. The terms used in the law include: collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, evaluation or control of information, modification, communication, transfer, dissemination, or extraction.

In practice, any action taken with personal data falls under this definition. Whether you are receiving, storing, sending, or analyzing data, you are engaging in data processing as part of your daily workflow. These examples are simply different forms of the broader concept of processing, which includes every possible interaction with personal data.

Even if you receive a physical medical record and store it in a drawer, that still counts as an activity involving personal data processing. The GDPR applies not only to digital data, but also to physical records. Therefore, for each data processing activity, it is essential to determine the most suitable legal basis for that specific action.

What are legal bases?

Legal bases are the legal justifications for processing of personal data in compliance with the GDPR. Data may only be used if its processing is justified by one of these legal bases, which is why they are so important.

The Brazilian GDPR allows for data processing under several different circumstances. There are 10 legal bases for the processing of general (nonsensitive) personal data and 8 legal bases specifically for the processing of sensitive personal data, as shown in Table 1.

The most well-known legal basis is consent, which refers to the unequivocal indication of the data subject's will to authorize the use of their data. Despite its popularity, consent is not necessarily the most suitable legal basis in all situations – in fact, in many practical scenarios, avoiding it is preferable. For instance, you are likely aware that medical records must be stored for a minimum of 20 years if they are in physical (paper) format.[2,3] Law No. 13.787/2018 allows for the destruction of physical or digitized records after 20 years; however, CFM Resolution No. 1.821/2007 establishes a different rule, requiring permanent storage of digitized or microfilmed records. As a result,

Table 1
Legal bases for general and sensitive personal data

General personal data	Sensitive personal data
Consent	Consent
Compliance with legal or regulatory obligations	Compliance with legal or regulatory obligations
Execution of public policies provided for in laws and regulations or supported by contracts, agreements, or similar instruments	Execution of public policies provided for in laws or regulations
Research conducted by a research body	Research conducted by a research body
Execution of a contract or preliminary procedures related to a contract to which the holder is a party, at the request of the data subject.	–
Regular exercise of rights in judicial, administrative, or arbitration proceedings	Regular exercise of rights, including in contracts and in judicial, administrative, or arbitration proceedings
Protection of the vital interests of the data subject or another natural person	Protection of the vital interests of the data subject or another natural person
Health protection	Health protection
Legitimate interests pursued by the controller or by a third party	–
Credit protection	Prevention of fraud and security of the data subject, in the processes of identification and authentication of registration in electronic systems

it is the Data Protection Officer (DPO)'s responsibility to analyze the applicable regulation in each case to determine the appropriate retention period.

Therefore, consent is not a suitable legal basis for the storage of medical records, as the data must be retained regardless of whether the patient consents, making consent irrelevant in such contexts. In these cases, the suitable legal basis would be "compliance with a legal or regulatory obligation." Another commonly used legal basis in health care is "execution of a contract." Often, it is necessary to use patient data to fulfill a contract – either directly with the patient or through a health insurance provider involved in the service.

Additionally, patient records may be used for legal defense in judicial proceedings, such as in cases involving allegations of medical error. The Medical Code of Ethics[4] permits the breach of medical confidentiality for justified reasons or with the patient's prior consent (Articles 73 and 89). The Brazilian GDPR also recognizes that sensitive data may be used in legal actions to exercise rights when the data subject is a party to the case. In such instances, there is legal support for using medical records in court, but several rules must be followed to ensure proper handling.

Another frequently used legal basis in medical settings is "health protection." This is often the most suitable basis for activities performed by health care professionals, health care services, or public health authorities. However, to rely on this basis, the processing of data must be conducted by licensed health professionals who are subject to confidentiality obligations imposed by their respective regulatory boards – such as the Federal Boards of Medicine, Pharmacy, or Nursing.

Another relevant legal basis is "legitimate interests." This can be applied in cases involving support or promotion of your clinic's activities. For example, with appropriate safeguards, you may use patients' email addresses to send relevant updates or informational content. It is important to note, however, that this basis cannot be used for processing sensitive personal data, such as health information from medical records, for marketing purposes or the interests of third parties.

Finally, when dealing with the data of children and adolescents, the Brazilian GDPR establishes a special legal framework that offers a higher level of protection. Legal bases in these cases are more restrictive, and all processing must prioritize the best interests of the child or adolescent.

Evaluating and applying legal bases is a complex task that should be undertaken by a qualified specialist. Beyond determining which legal basis is suitable for each activity, the professional must also be capable of structuring the entire data processing infrastructure to ensure full compliance with the GDPR.

Physician responsibilities

Noncompliance with the GDPR can lead to significant financial penalties for physicians, as well as serious reputational damage and loss of patient trust. For this reason, compliance with the law is essential to prevent such consequences. Below is a breakdown of the main areas of legal responsibility.

Administrative responsibility

The first type of liability under the Brazilian GDPR is administrative, meaning it arises from noncompliance with the law and falls under the oversight of the ANPD. Violating the GDPR can subject private medical practices to sanctions ranging from warnings to fines of up to 2% of the organization's gross revenue from the previous fiscal year (excluding taxes), capped at R$ 50,000,000.00 per infraction.[5]

While the risk of a fine may seem alarming, it is also important to consider that other penalties may apply – such as the partial or total suspension of activities involving personal data processing. In these cases, you will be prohibited from processing data, which could mean the inability to perform your professional activities. Furthermore, even if a sanction is later overturned, the reputation of your clinic may be harmed.

Another form of administrative responsibility, although not directly linked to data protection, may arise through professional oversight bodies, such as the Federal and Regional Medical Boards. There have already been cases of disciplinary actions, such as by the Regional Medical Board of Ceará (CREMEC),[6] where a physician displayed identifiable clinical cases and patient images in professional advertisements. In this case, inadequate handling of personal data led to an administrative penalty and revocation of the physician's license.

Judicial responsibility

Physicians may also face judicial (civil) liability. This applies in situations where, through action or omission, negligence, or recklessness, one person causes harm to another. In such cases, civil damages – whether compensatory or general – are awarded to the harmed party.

The extent of this liability will be determined by the judge if the patient feels harmed. In data protection scenarios, legal action may be taken if a data breach exposes a patient's sensitive data. If such a breach results in harm to the patient's reputation or leads to discrimination, the physician may be held legally responsible.

Although difficult to quantify, civil damages awarded in similar scenarios can serve as reference for estimates. For instance, in cases involving financial institutions, the Court of Justice of Minas Gerais has typically awarded general damages averaging BR 8,000.00.[7] While the circumstances differ from those involving medical professionals, judges may reference such amounts in cases of GDPR violation.

In addition to general damages, if the patient demonstrates that financial losses have also occurred, compensatory damages may also be awarded as a result of inadequate data processing.

Contractual responsibility

A third type of liability arises from contractual obligations. If you work with health insurance providers, you have likely signed an affiliated provider agreement that outlines specific data protection responsibilities. Even in private agreements, similar clauses may exist, including penalties for noncompliance.

Regardless of the contract, safeguarding patient data is a legal obligation, and failing to do so may be deemed a breach of contract. This means that any damages or losses caused by such failure may result in the application of penalties.

In the face of risk and uncertainty, what should be done? How to comply with the GDPR?

Complying with the Brazilian GDPR in medical practice is a multidisciplinary effort that requires collaboration among professionals from different fields. The objective is to ensure adequate protection of patient data.

It should be noted that compliance with data protection regulations cannot be achieved through a one-time effort, such as merely publishing a privacy policy on the clinic's website. Because data processing is a continuous, day-to-day activity, the compliance process must also be ongoing. For this reason, the most effective way to meet the requirements of the Brazilian GDPR is to establish a permanent Data Governance Program. This program should be managed by a DPO, who can be either a natural person (individual) or a legal entity (company or law firm). The key role of the DPO is to continuously monitor the practice's data processing activities.

In addition to preparing and providing standard documents, the DPO should also be able to identify the applicable legislation, monitor ongoing legal updates, and ensure the practice remains compliant – while also identifying opportunities for improvement. The work performed may vary depending on the size and needs of the practice, but generally follows a structured set of phases, as outlined below.

Documentation of data processing activities

Documenting a data processing operation is similar to creating a Standard Operating Procedure (SOP). An SOP is a document that describes, in detail, the steps required to perform a specific task in the medical office. It serves as a standardized protocol designed to ensure consistency, allowing any team member to follow the procedure correctly. SOPs may cover a wide range of procedures, from patient care workflows to hand-washing techniques.

As part of the Data Governance Program, the DPO is responsible for documenting all internal processes of the clinic: from patient care workflows to administrative operations. For each process, the DPO will specify which data are being processed, who has access to the data, where the data are stored, what security measures are in place, and any other relevant details necessary to understand the complete lifecycle of personal data.

Conduction of diagnostic assessment

After mapping all data flows – a process that serves as a "snapshot" of how personal data are handled in the clinic – a diagnostic assessment should be conducted in accordance with the Brazilian GDPR. One of the main actions during this phase is the selection of a legal basis for each data processing

activity. This step is especially important because, as previously mentioned, no data processing may occur without a valid legal basis, under penalty of violating the GDPR.

This phase should also include a risk classification of each process. According to ANPD Resolution 02/2022, processes may be considered high-risk if they: (a) Involve the processing of a large volume of personal data, (b) pose a risk to fundamental rights and freedoms, (c) involve the use of innovative technologies, surveillance technologies, or automated processes, or (d) involve data of children or older adults.

It is important to note that this analysis is not straightforward, as many uncertainties remain. For example, the definition of what constitutes a "large volume" of data is still being developed by the ANPD, and there is no objective benchmark yet for how many patients would qualify a practice as "handling a high volume." Therefore, it is strongly recommended that this diagnostic evaluation be performed by the DPO.

Gap identification and risk mitigation

Both the documentation of data processing activities and the performance of a diagnostic assessment are not only mandatory under the Brazilian GDPR but also play a critical role in identifying procedural gaps and mitigating risks. For instance, when mapping the patient care workflow, the DPO may discover that patient records are being stored in an unlocked drawer. This storage method leaves sensitive data vulnerable to unauthorized access. The DPO might recommend installing locks or safes to create a physical layer of data security.

Another common gap in medical practices is data duplication. For example, patient documents might be saved simultaneously on a local computer, email inbox, cloud drive, and also printed on paper. While this may seem to provide additional security, it can actually increase the risk of data breaches – such as unauthorized data access by a third party –, especially when there is no centralized control over where and how the data are stored.

Challenges and precautions in implementing a Data Governance Program for physicians

Implementing a Data Governance Program presents challenges across all sectors. Mapping every process, identifying risks, and implementing corrective measures are tasks that demand precision and care.

In the medical field, the implementation of such a program requires special attention in specific areas. For the purposes of this article, two key focus points will be discussed: storage of electronic medical records and the physician's relationship with health insurance providers.

Electronic Patient Records (PEP) and Electronic Health Records (EHR)

The digital transformation of health care has become increasingly prominent. As digital technologies evolve, traditional paper documents that once structured patient information, such as medical records, have become digitalized.

On the one hand, this transformation has brought numerous benefits in terms of data accessibility for both physicians and patients. On the other hand, it has introduced redundancy between physical and digital files, along with security risks.[8] In many cases, physical copies of digitized documents continue to be stored in boxes or filing cabinets without adequate control, increasing the risk of unauthorized access. Additionally, the law mandates retention periods for these documents, after which they must be destroyed. Without active oversight, there is a risk that these documents will be improperly stored indefinitely.

If it comes as a surprise that personal data are subject to a retention period, it is important to understand that all data processing must be tied to a specific purpose. Data may only be used as long as necessary to fulfill the stated purpose. Once that purpose is achieved, the data must be deleted, or the organization may be found in violation of the GDPR.

For example, consider a situation in which you have concluded care for a patient, with no ongoing treatment plans, and the patient's file has not been accessed for some time. One could say that the purpose for processing the data has ended, and this could justify shredding the physical medical record. However, Law No. 13,787/2018 requires that paper medical records be retained for a minimum of 20 years from the date of the last entry. After this period, the data must be destroyed, as the legal purpose for its retention would also have ended.

Just like medical records, all documents in a medical practice are subject to specific retention periods. Analyzing these timelines and developing a

records retention schedule is one of the responsibilities of the DPO.

Another important DPO task related to electronic records is the evaluation of software vendors. It is common in the medical field to use software platforms for the management of medical records. However, selecting a platform that does not comply with the Brazilian GDPR requirements can result in legal liability for the physician, as discussed in the "Physician responsibilities" section. Therefore, before signing any contract with a vendor, it is essential to conduct a thorough assessment of the company – known as vendor due diligence – based on a checklist of GDPR requirements. This evaluation determines the vendor's maturity in data protection practices and helps to identify potential risks associated with the partnership.

Relationship with health insurance providers

Another important challenge for physicians involves their interactions with health insurance providers. Typically, the affiliation agreements signed with these providers include specific data protection clauses that establish mutual responsibilities. As a result, a physician working with multiple providers will be subject to different contractual obligations related to data protection.

For example, a contract with Provider X may stipulate that, in the event of a data security incident, the physician must notify the provider and take appropriate action within 72 hours. Meanwhile, a contract with Provider Z may impose a stricter deadline of 24 hours for the same actions. Therefore, it is important that the physician maintain strict control and awareness of these obligations to avoid violating contractual terms.

Some health insurance providers may also require that patient documents be stored in accordance with specific standards, such as using segregated databases. When reviewing the agreement, the DPO can identify such obligations and, if necessary, perform a risk analysis of the clauses.

For this reason, it is strongly recommended that physicians carefully review all data protection clauses during the affiliation process with any health insurance provider.

Liability insurance

Liability insurance is a form of financial protection that professionals, including physicians, can acquire to protect themselves against civil liability claims and the costs associated with legal proceedings. This insurance typically covers legal defense costs, compensations, and settlements arising from allegations of medical negligence.

Insurance options for physicians

As is well known, physicians face a variety of risks in their daily practice that can affect both their professional careers and their patients' well-being. These risks may range from medical errors (which can lead to lawsuits) to failures in the IT security infrastructure of clinics and offices. In this context, insurance coverage for physicians is highly recommended, as it provides both financial and professional protection, in addition to offering greater peace of mind and security in the practice of medicine.

There are several types of insurance that can help health care professionals feel more secure in their work. Among the most relevant are the following:

– *Professional liability insurance:* designed to protect physicians against claims of damage caused by errors, omissions, or negligence in the practice of medicine. It typically covers legal expenses, compensation payouts, and other costs related to legal proceedings.
– *Equipment insurance:* covers damage or loss of medical equipment due to theft, fire, or other unexpected events.
– *Health and life insurance:* provides financial protection for physicians and their families in the event of serious illness, accidents, or death.
– *Cyber insurance:* covers risks related to information technology and data privacy. This type of insurance helps physicians manage the consequences of cyber incidents, such as data breaches, ransomware attacks, or security violations.

Given the increasing relevance of cyber threats, it is worth taking a closer look at cyber insurance.

Cyber insurance

With the increasing digitalization of health care, cybersecurity has become a central concern. As discussed earlier, patient data is both sensitive and valuable, making it a frequent target of cyberattacks. In addition, data breaches can result in serious legal and financial consequences for physicians and their practices, as well as cause significant reputational harm.

To prevent these risks, it may be worthwhile to invest in a good cyber insurance policy, which typically covers the following:

– Incident response costs: covers the expenses involved in responding to a cyberattack, including hiring IT specialists to contain and resolve the issue.
– Notification and credit monitoring: includes the costs of notifying patients about a data breach and offering credit monitoring services to prevent fraud.
– Data privacy and security liability: protects against legal actions and fines resulting from failure to properly secure personal data.
– Revenue loss and data recovery: compensates for lost income due to operational disruptions and covers the cost of restoring lost or compromised data.

Physicians should view cyber insurance as an essential component of their risk management strategy. With the widespread use of EHRs and digital patient management systems, the likelihood of suffering a cyberattack is significantly increased.

By investing in comprehensive coverage, physicians can focus on what they do best – caring for their patients – while remaining protected from the multiple risks associated with their profession.

Conclusion

The GDPR has introduced a new paradigm for the processing of personal data in Brazil, significantly impacting a range of sectors – including health care. Medical practices, which handle a wide array of patient information on a daily basis, must adapt to this legislation to ensure adequate data protection and to avoid serious consequences.

As outlined, personal data refers to any information related to an identified or identifiable natural person, while sensitive data includes information that may lead to discrimination, such as racial or ethnic origin, religious beliefs, political opinions, and health information. The Brazilian GDPR places an additional layer of protection on sensitive data, strictly limiting the circumstances under which they can be processed.

Personal data processing is a relevant concept that encompasses a wide range of activities, from data collection and storage to data processing and sharing. Each of these actions must be supported by a valid legal basis. In the medical field, the most relevant legal bases include patient consent, compliance with a legal or regulatory obligation, execution of a contract, and health protection. Choosing the correct legal basis is crucial, as an incorrect choice may lead to GDPR violations.

Physicians must be aware of the administrative, judicial, and contractual responsibilities that may arise from noncompliance. Administratively, the ANPD may impose sanctions ranging from warnings to significant fines, or even suspend data processing activities. Judicially, civil liability may lead to claims for general or compensatory damages, depending on the consequences of a data breach or misuse. Contractually, penalties may be enforced if data protection clauses are breached.

To mitigate these risks and ensure compliance, it is essential to implement a Data Governance Program. Such program must be ongoing and include continuous monitoring of data processing activities, the establishment of appropriate security measures, and the detailed documentation of processing operations. The DPO plays a key role in this process, ensuring that all activities are in line with the applicable legislation.

Moreover, the digitalization of medical records, such as PEPs and EHRs, demands special attention. Choosing vendors that comply with the Brazilian GDPR and managing the data lifecycle effectively are key steps in preventing breaches and ensuring patient privacy.

In conclusion, GDPR compliance presents a complex and ongoing challenge for medical practices. However, by implementing a robust governance program and adopting proper security practices, clinics can effectively protect patient data, avoid penalties, and build trust in their services. Investing in compliance not only prevents legal sanctions but also fosters ethical and responsible medical practice, ultimately benefiting both healthcare professionals and their patients.

References

1. Brasil. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, p. 1, 15 agosto de 2018.
2. Brasil. Lei nº 13.787, de 27 de dezembro de 2018. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuários de pacientes. Diário Oficial da União: seção 1, Brasília, DF, 28 dez. 2018.

3. Conselho Federal de Medicina, Brasil. Resolução CFM n° 1.821, de 11 de julho de 2007. Define prontuário médico e estabelece normas gerais para o manuseio, a guarda e o sigilo de informações de saúde. Diário Oficial da União: seção 1, Brasília, DF, p. 205, 22 de agosto de 2007.
4. Conselho Federal de Medicina, Brasil. Código de Ética Médica: Resolução CFM nº 2.217, de 27 de setembro de 2018. Brasília, DF: CFM, 2018.
5. Autoridade Nacional de Proteção de Dados, Brasil. Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023. Publica regulamento de dosimetria [Internet]. Available from: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon4CDANPD24.02.2023.pdf. Accessed on May 27 2024.
6. Conselho Federal de Medicina, Brasil. Publicidade Médica: Justiça mantém decisão do CFM e do Cremec contra médico que violava preceitos éticos [site na Internet]. Available from: https://portal.cfm.org.br/noticias/publicidade-medica-justica-mantem-decisao-do-cfm-e-do-cremec-contra-medico-que-violava-preceitos-eticos/. Accessed on May 24 2024.
7. Minas Gerais, Brasil. Tribunal de Justiça. 18ª Câmara Cível. Apelação cível nº 1.0000.23.240968-0/001. Julgado em 2023.
8. Costa JAF. Tratamento e transferência de dados de saúde: limites ao compartilhamento de dados sensíveis. In: Dallari AB & Monaco GFC, eds. LGPD na Saúde. São Paulo: Thomson Reuters; 2021. p. 89.

No conflicts of interest declared concerning the publication of this article.

Corresponding author:
Eduardo Magalhães de Souza Lima
E-mail: eduardo@souzalima.med.br