Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitario
ISSN: 2358-1824

Article

Challenges in implementing the General Data Protection Law in telehealth services: an integrative review

Desafios da implementação da Lei Geral de Proteção de Dados em serviços de saúde que fazem uso da telemedicina: uma revisão integrativa

Desafíos en la implementación de la Ley General de Protección de Datos en servicios de telemedicina: una revisión integrative

Eloísa Karine Braga Lopes[1]
Fundação Oswaldo Cruz, Brasília, DF.
https://orcid.org/0009-0000-1402-3535
eloisa.bcastro@gmail.com

Filipe Henrique Lopes[2]
Faculdade Minas Gerais, Belo Horizonte, MG.
https://orcid.org/0009-0007-0746-2047
fhlopes16@gmail@gmail.com

Nínive Aguiar Colonello[3]
Ministério da Saúde, Brasília, DF.
https://orcid.org/0000-0003-4684-9977
nicolonello@gmail.com

Fernando Passos Cupertino de Barros[4]
Universidade Federal de Goiás, Goiânia, GO.
https://orcid.org/0000-0003-1188-7973
fernandocupertino@gmail.com

Renato Silva Avelar[5]
Secretaria Municipal de Saúde, Goiandira, GO.
https://orcid.org/0000-0001-7428-6126
renato.avelar30@gmail.com

Submitted on: 08/19/24
Revision on: 10/07/24
Approved on: 10/13/24

Abstract

Objective: To investigate the challenges and opportunities of implementing the General Data Protection Law in health services using telemedicine, aiming to identify gaps and suggest improvements and public policies. **Methodology:** An integrative review was conducted, selecting articles from databases such as Virtual Health Library, CAPES Journals, Luiz Viana Filho Academic

[1] Medical, Universidade do Rosário Vellano, Belo Horizonte, MG, Brazil. Student, Fundação Oswaldo Cruz, Brasília, DF, Brazil.
[2] Bachelor of Business Administration, Pontifícia Universidade Católica, Belo Horizonte, MG, Brasil. Student, Faculdade Minas Gerais, Belo Horizonte, MG, Brazil.
[3] Ph.D in Sciences, Universidade de São Paulo, Ribeirão Preto, SP, Brazil. Tecnologista Plena, Ministério da Saúde, Brasília, DF, Brazil.
[4] Ph.D in Public Health, Universidade de Brasília, Brasília, DF, Brazil. Professor, Universidade Federal do Goiás, Goiânia, GO, Brazil.
[5] LL.M in History, Universidade Federal de Catalão, Catalão, GO, Brazil. Coordinator of the Environmental Health and Surveillance, Secretaria Municipal de Saúde, Goiandira, GO, Brazil.

Library, and PubMed, using descriptors like “telemedicine”, “telehealth”, “general data protection law”, “data protection”, and “health”. **Results:** The analysis highlighted the need for health information systems to adapt to General Data Protection Law compliance, underlining challenges such as implementing informed consent and information security measures. Opportunities include increasing patient trust in telehealth services and innovating data management practices. **Conclusion:** Effective implementation of the General Data Protection Law in the health sector requires a multifaceted approach that includes technological and procedural adjustments and a commitment to the continuous education of healthcare professionals. This is crucial for ensuring the security of patient data, promoting privacy, and driving innovation in digital health.
Keywords: Telemedicine; Data Protection; Digital Health; Health Personnel.

Resumo

Objetivo: Investigar os desafios e oportunidades da implementação da Lei Geral de Proteção de Dados em serviços de saúde que utilizam a telemedicina, visando identificar lacunas e sugerir melhorias e políticas públicas. **Metodologia:** Foi realizada uma revisão integrativa, selecionando artigos das bases de dados Biblioteca Virtual de Saúde, CAPES Periódicos, Biblioteca Acadêmica Luiz Viana Filho e PubMed, utilizando os descritores "telemedicina", "telessaúde", "Lei Geral de Proteção de Dados", "proteção de dados" e "saúde". **Resultados:** A análise evidenciou a necessidade de adaptação dos sistemas de informação em saúde para a conformidade com a Lei Geral de Proteção de Dados, destacando desafios como a implementação de consentimento informado e medidas de segurança da informação. As oportunidades incluem o aumento da confiança dos pacientes nos serviços de telessaúde e a inovação em práticas de gestão de dados. **Conclusão:** A implementação eficaz da Lei Geral de Proteção de Dados no setor de saúde exige uma abordagem multifacetada que inclua ajustes tecnológicos, processuais e um compromisso com a educação contínua dos profissionais de saúde. Isso é crucial para garantir a segurança dos dados dos pacientes, promovendo a privacidade e impulsionando a inovação em saúde digital.
Palavras-chave: Telemedicina; Proteção de dados; Saúde digital; Pessoal de saúde.

Resumen

Objetivo: Investigar los desafíos y oportunidades de la implementación de la Ley General de Protección de Datos en servicios de salud que utilizan la telemedicina, con el fin de identificar lagunas y sugerir mejoras y políticas públicas. **Metodología:** Se realizó una revisión integrativa, seleccionando artículos de bases de datos como Biblioteca Virtual de Salud, Periódicos CAPES, Biblioteca Académica Luiz Viana Filho y PubMed, utilizando descriptores como "telemedicina", "telesalud", "ley general de protección de datos", "protección de datos" y "salud". **Resultados:** El análisis resaltó la necesidad de adaptación de los sistemas de información en salud para la conformidad con la Ley General de Protección de Datos, destacando desafíos como la implementación del consentimiento informado y medidas de seguridad de la información. Las oportunidades incluyen el aumento de la confianza de los pacientes en los servicios de telesalud y la innovación en prácticas de gestión de datos. **Conclusión:** La implementación efectiva de la Ley General de Protección de Datos en el sector de la salud requiere un enfoque multifacético que incluya ajustes tecnológicos, procesales y un compromiso con la educación continua de los
profesionales de la salud. Esto es crucial para garantizar la seguridad de los datos de los pacientes, promoviendo la privacidad e impulsando la innovación en la salud digital.

Palabras clave: Telemedicina; Protección de Datos; Salud Digital; Personal de Salud.

Introduction

Telemedicine has emerged as an innovative way of providing services, enabling patients to access medical treatment remotely. Increasingly used and widespread, this type of care has also raised important questions about the protection of sensitive data of users of this technology[1].

We live in a historical moment of great technological evolution, in which the search for and availability of information is ever increasing[1]. In response to social needs, the digital transformation is moving towards reducing barriers and providing unprecedented access to information, education and health. As digital health advances, increasingly elaborate and systematized measures are needed to protect the binomial of data security and privacy[2].

In Brazil, Law Nº. 13.709/2018 - the General Data Protection Law (LGPD) - has the role of regulating the use of data, ensuring technological development without infringing fundamental and inalienable rights. It can be seen not only as a regulatory norm, but also as part of Human Rights, since its correct execution has the power to inhibit discriminatory acts resulting from data leaks[2].

The LGPD is a reflection of an international movement to uphold the rights to personality, image, honor and dignity[2,3].

It will be possible to achieve a complete coverage of the LGPD when there is a standardization of models for collecting and using information or a broadening of the interpretation of the Law, allowing it to be adapted to the different particularities of the systems. Legal norms need to be reviewed periodically in view of the speed with which information and communication technologies advance and digital health expands[1].

The integration of telemedicine into healthcare services represents a milestone in the technological advancement of the sector, offering practical solutions for accessibility to medical care. However, this evolution brings with it the responsibility of guaranteeing the security and privacy of patient data, especially in a scenario where most interactions take place on digital platforms. The LGPD is a fundamental instrument in the legal framework that aims to protect personal and sensitive data, imposing a challenge for healthcare professionals and institutions that adopt telemedicine: that of aligning technological operations and data management processes with legal compliance. Adhering to these standards not only safeguards patient information, but also strengthens confidence in the use of telemedicine as a safe and efficient means of providing health services[1].

The article therefore presents an analysis, based on an integrative literature review, of the challenges and opportunities of implementing the General Data Protection Law in health services that use telemedicine.

Methodology

This was an integrative review with the aim of identifying the challenges and opportunities of implementing the General Data Protection Law in health services that use telemedicine.

The following databases were used to search for the articles: Biblioteca Virtual de Saúde <https://bvsalud.org/>, CAPES Periódicos <https://www-periodicos-capes-gov-br.ezl.periodicos.capes.gov.br/>, Biblioteca Acadêmica Luiz Viana Filho

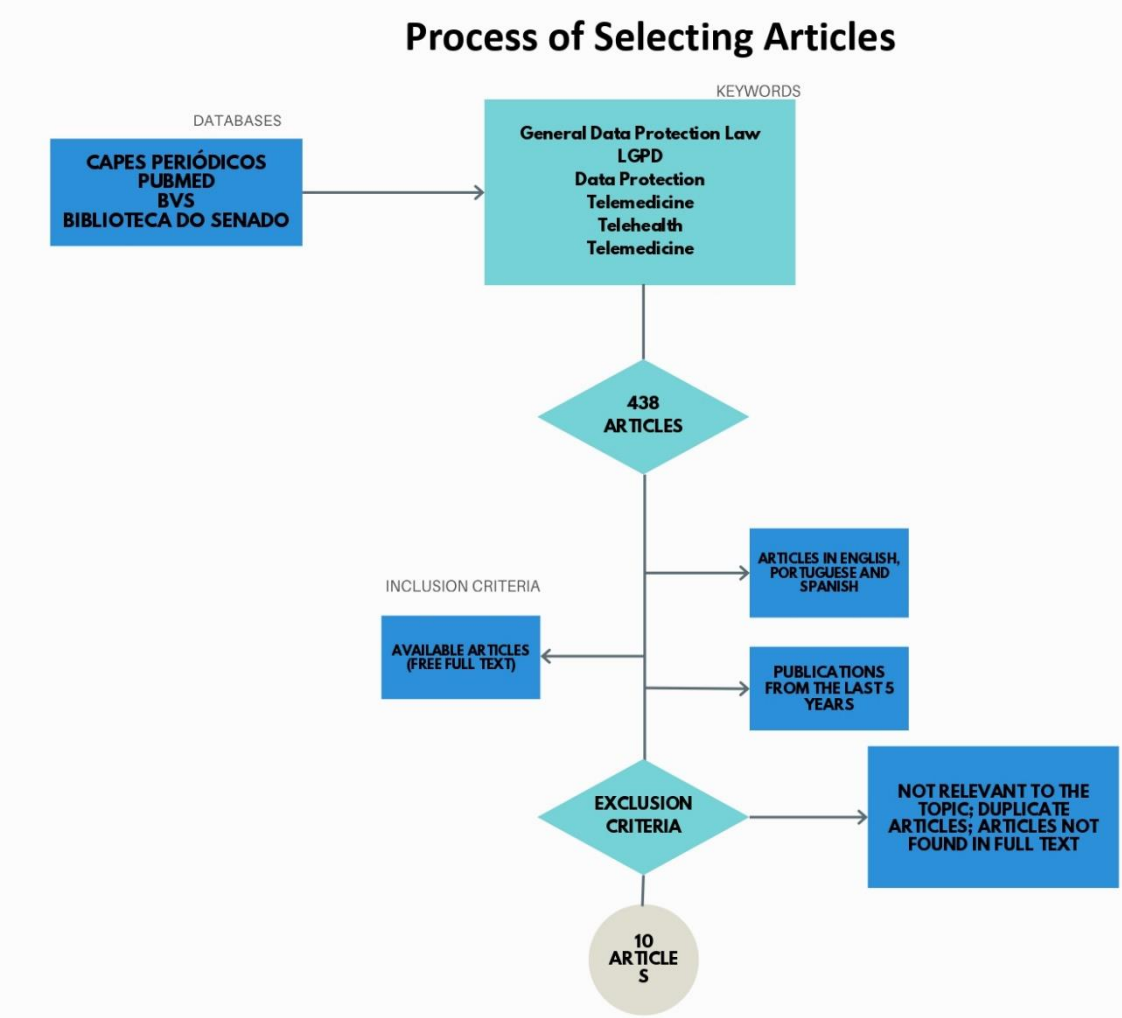
<https://www2.senado.leg.br/bdsf/item/id/70371> and *PubMed* <https://pubmed.ncbi.nlm.nih.gov/>. These databases were selected because of their relevance and scope in the field of health and health law.

The search strategy was developed with the aim of identifying articles relevant to the research topic. The descriptors used were: “telemedicine”, “telehealth”, “general data protection law”, “data protection” and “health”. These descriptors were combined using the Boolean operators “AND” and “OR” to broaden the scope of the research.

Inclusion and exclusion criteria were established for the selection of articles. The inclusion criteria were: (1) articles published in the last five years and (2) written in Portuguese, English or Spanish. The exclusion criteria were: (1) articles not available in full, (2) duplicates, (3) unrelated to the research topic and (4) analysis of cases from other countries.

Initially, the search in the databases resulted in a total of 438 articles (Figure 1). After applying the exclusion criteria, 10 articles were selected for the integrative review. The articles were selected by two independent reviewers, with any discrepancies being resolved by a third reviewer.

Figure 1. Flowchart for searching articles in databases



Source: Prepared by the authors, 2024

Results and discussions

Faced with the implementation of the General Data Protection Act (LGPD)[3] in the context of telehealth, a series of challenges have arisen for healthcare professionals, marking a significant transformation in the way patient data is handled and protected. Analysis of the selected articles reveals various dimensions of these challenges, as well as opportunities to improve telehealth practice under the new legal framework[1,2].

Box 1. Main characteristics of the articles studied

Article	Authors	Year	Scientific Journal	Type of Study	Main results
Pesquisa com prontuário: análise ético-jurídica à luz dos Direitos Humanos dos Pacientes	Aline Albuquerque[5]	2019	Cadernos de Ética em Pesquisa	Investigative research	The right to privacy and confidentiality is essential in research with human beings.
Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde	Suéllyn Mattos de Aragão, Taysa Schiocchet[1]	2020	Revista Eletrônica de Comunicação, Informação e Inovação em Saúde (RECIIS)	Qualitative, descriptive and exploratory research	SUS needs to adapt to the LGPD.
Lei Geral de Proteção de Dados e segurança da informação na área da saúde	Renata Salgado Leme, Marcelo Blank[6]	2020	Cadernos Ibero - Americanos de Direito Sanitário	Exploratory bibliographical and documentary research	The widespread use of digital media in healthcare exposes patients to privacy risks.
Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global	Bethania de Araujo Almeida et al.[7]	2020	Ciência & Saúde Coletiva	Reflective analysis	The right to privacy and the protection of personal data are fundamental in the fight against the pandemic.
Privacidade e confidencialidade das informações clínicas em saúde mental: velhos desafios em um novo contexto	Ana Cristina Tietzmann et al.[8]	2021	Brazilian Journal of Psychotherapy	Narrative review	Increased need for data protection in mental health in the digital age.

Internet das Coisas e blockchain no Sistema Único de Saúde: a proteção dos dados sensíveis diante da Lei Geral de Proteção de Dados	Maria Amália Arruda Camara et al.[9]	2021	Cadernos Ibero - Americanos de Direito Sanitário	Narrative review	Lack of transparency in the processing of personal data and little accountability.
Questões éticas e perspectiva jurídica da proteção de dados	Edith Maria Barbosa Ramos et al.[10]	2021	Cadernos Ibero - Americanos de Direito Sanitário	Deductive, descriptive research	Analysis of the new model for protecting the use of data in research and by the Public Administration.
Por uma transformação digital que assegure o direito à saúde e à proteção de dados pessoais	Hêider Aurélio Pinto et al.[11]	2022	Saúde em Redes	Reflective analysis	Progress in health services through digitalization and the emerging need for data governance.
A Lei Geral de Proteção de Dados e suas implicações na saúde: as avaliações de impacto no tratamento de dados no âmbito clínico-hospitalar	Margareth Vetis-Zaganelli, Douglas Luis Binda Filho[12]	2022	Revista de Bioética y Derecho	Literature and document review	There is a lack of definition in the LGPD as to whether health impact assessments are mandatory.
Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital	Siderly do Carmo Dahle de Almeida, Tania Aparecida Soares[13]	2022	Perspectivas em Ciência da Informação	Documentary research	The LGPD has brought about a change in culture, adding greater responsibility to the processing of personal data

Source: The authors (2024)

Câmara and collaborators[9] show weaknesses in the privacy of SUS users' health information and propose improvements through personal data storage or the use of blockchain to overcome vulnerabilities and maintain the secrecy of sensitive information. It reports that, with the entry into force of the LGPD, special attention has been paid to the treatment of personal data, especially sensitive data, protecting individual rights and guarantees, focusing on information security and establishing data governance that advocates the preservation of privacy. The argument is raised that blockchain can provide solutions in terms of integrity, certification and availability by decentralizing information and overcoming potential vulnerabilities. However, a disadvantage of the blockchain tool that needs to be taken into account is that once data is entered into the network, it is practically impossible to rectify or withdraw the data, which hurts the exercise of the data subject's rights, concerning the right to rectify inaccurate data, the right to delete data by withdrawing consent and especially the right to forget data, which must be deleted by blockchain developers.

Personal data storage can be seen as an interesting strategy for storing, managing and deploying personal data in a secure and structured way. Users have ownership of their personal data, increasing their empowerment over their own data by being able to define which services can access it and which data can be retrieved by each service. Access to their data is done through granular permissions so that sharing is managed by the data owner. Camara and collaborators[9] suggest that personal data storage can be adopted for sensitive data from health services, reinforcing the right to data privacy.

Ramos and collaborators[10] point out that the LGPD has brought advances to the protection of sensitive data, emphasizing that the LGPD has consequences for human health research for the actors involved, providing rules for the use of sensitive data, anonymization and the authorization of the data subject to carry out health treatments.

The LGPD establishes that the processing of personal data can be carried out for the protection of health in procedures carried out by health professionals, health services or the health authority . Communication or shared use between data controllers is permitted for the provision of health services, pharmaceutical assistance and health care.

The LGPD prohibits the use of data for the purposes of selecting users for private health plans, hiring and excluding beneficiaries by health operators. Exceptional cases include auxiliary diagnostic and therapy services, and data portability is allowed when requested by the data subject.

The new legislation calls for personal data to be anonymized whenever possible and also stipulates that the dissemination of public health research results should not reveal personal data, with the research institution being responsible for the security of the information and the transfer of data to third parties being prohibited. The LGPD also establishes that personal data must be kept in a controlled and secure environment and eliminated after the end of processing, although the retention of data for studies by research bodies is authorized. Data used in research should be anonymized or pseudo-anonymized whenever possible, following the ethical standards of studies and research.

The LGPD created new rights with the aim of guaranteeing data subjects that their personal data will be processed properly, responsibly and securely. The law has brought significant progress in terms of establishing new responsibilities and obligations for data controllers and operators.

As reported by Pinto and collaborators[11], the LGPD brought about significant changes aimed at protecting personal data, defining this protection as a citizen's right. The LGPD also protects against the misuse of personal data, such as the use of personal data for economic purposes, and aims to

guarantee citizens' privacy and control over their data. The authors also report on the importance of not giving up on exercising data protection and implementing digital transformation in the Brazilian health system, so that these two aspects need to be carried out in a joint and integrated manner, seeking data governance that promotes transparency and compliance with the LGPD, especially with regard to recognizing data protection as a fundamental right.

They also report that it is essential to build policies and strategies that make data protection and security effective and point out that the LGPD needs to be improved to regulate and discipline the actions of the private sector, in order to make it impossible to share and sell data improperly, as well as to subject companies that practice segmentation and adverse customer selection actions to sanctions, disrespecting criteria of equality and fairness.

They also point out that there needs to be improvements in the supervision and qualification of legislation to curb the misuse of data, such as, in the health sector, avoiding the indication of unnecessary procedures, exams and medicines in the interests of those who make a profit from them, the exclusion or adverse selection of users of health plans, by projecting expenses above the average costs for users. The authors defend the idea of following a model based on autonomy and control over data by the citizen, who is the owner of the data and has awareness and control over the use of their data. They believe it is urgent to increase and guarantee the protection of personal data by implementing and improving the LGPD with regard to the inappropriate and harmful commercial use of data.

Zaganelli & Binda Filho[12] discuss the inaccuracies of the LGPD in relation to the preparation of impact reports to analyze the processing of data by health institutions that generate large amounts of sensitive data. They also point out gaps in the LGPD such as: i) disproportionality for benefiting its implementation by large companies due to its high cost of compliance; ii) lack of mention of the need to formalize the link between operator and controller; iii) lack of identification of cases in which impact reports are required; iv) lack of specific deadlines for communication in cases of security incidents that may entail risk or harm to data subjects; v) lack of express mention of what would be "best interests" with regard to the processing of minors' data; vi) lack of a defined deadline for notifying the authority of the risk of data leakage; vii) subjectivity in defining what constitutes a "reasonable" level of protection for personal data, which gives regulators significant flexibility in assessing fines for data breaches and/or non-compliance.

Impact reports are important tools in the execution of data management, ensuring that controllers do not violate the rights of data subjects, guaranteeing medical secrecy, confidentiality, privacy and patient safety. More specifically, the Personal Data Protection Impact Report (PDPIR) is an essential document in risk assessment processes for the processing of personal data that is collected, processed, used and shared. Following the risk assessment, measures are adopted to mitigate risks that could affect the civil liberties and fundamental rights of data subjects.

However, the obligation for impact reports is not explicitly stated in the LGPD. In the Law, there are only articles that define it and inform that the National Data Protection Authority - ANPD, in some cases may request these reports from controllers, but without specifying in which situations.

It is understood that the impact report is necessary when data processing involves sensitive data, even though the LGPD does not make it mandatory to carry out impact assessments when processing health data. The law only states that the ANPD may, in certain contexts, require the controller to carry out these reports. The authors point out that the processing of sensitive health data is likely to pose a

high risk to the rights of data subjects, and that it is essential to carry out impact assessments as part of governance processes.

Almeida & Soares[13] reflect on the objective of improving the governance of personal data by the various players who process data governed by the LGPD, in a scenario in which technological advances have made the information collected valuable assets from an economic perspective, and the protection of this information is a priority. Following the entry into force of the LGPD, institutions that process personal data, which makes it possible to identify a natural person, must comply with the law in order to protect the fundamental rights of privacy, ethics and freedom.

The hypotheses provided for in the law in which sensitive or non-sensitive data may be processed are highlighted, reinforcing the need for the consent of the data subject as a premise, except when it falls within the hypotheses in which consent may be waived. The LGPD prohibits the communication or shared use between controllers of sensitive personal data relating to health with the aim of obtaining an economic advantage, except in cases relating to the provision of health services, pharmaceutical assistance and health care, including auxiliary diagnosis and therapy services, for the benefit of the interests of the data subjects.

In addition to the regulations in place, the authors pointed out that the LGPD has led to a change in the culture of public and private institutions and organizations, encouraging greater responsibility and changing the way data is processed and handled with greater security, since it takes into account the possibility of data being misused for economic and commercial purposes.

A reflection is made on the applicability of the LGPD in Higher Education Institutions (HEIs) as data controllers, as they are called by law, in obtaining control and power over data processing, being responsible for compliance with personal data protection rules and for effectiveness and security measures, considering the principles of purpose, adequacy, necessity, free access, quality, transparency, security, prevention and non-discrimination.

HEIs, as data controllers, must adopt measures to guarantee the transparency of data processing based on their legitimate interests, as provided for in the LGPD. It is also necessary to guarantee cyber security to prevent possible data leaks by controllers, ensuring the privacy of data subjects.

The applicability of the LGPD to HEIs has changed the paradigm for concern about the ethical and secure use of personal data, protecting personality and privacy, so that HEIs must adjust through available technological tools, methodology and legal support in order to ensure the rights of data subjects in accordance with current guidelines.

In summary, the institutions that act as data controllers have challenges to overcome with the entry into force of the LGPD, such as raising awareness among data holders of ethical practices, making investments to create mechanisms and digital technologies to increase data security. In short, and more broadly, there is the challenge of establishing a program of good data governance practices that guarantees the adoption of institutional policies and processes that ensure the ethical and secure use of personal data.

In general terms, one of the main challenges identified is the need to adapt health information systems to ensure compliance with the principles and requirements of the LGPD. This includes implementing robust consent mechanisms, anonymizing data whenever possible, and adopting

effective information security measures to prevent leaks and unauthorized access. In addition, the legislation imposes the need for transparent and accountable data management, requiring

healthcare professionals and institutions to be able to inform patients about the use of their data, the rights of data subjects and how these rights can be exercised[1,2].

However, the transition to full GDPR compliance also opens up significant opportunities for improvement in telehealth. Enhanced protection of personal health data can increase patient confidence in the use of telehealth services, contributing to greater adherence to these modalities of care. In addition, compliance with the LGPD can stimulate innovation in data management practices, such as the development of more secure and efficient data storage and processing systems that not only protect patient privacy, but also facilitate data analysis for the continuous improvement of the quality of health services[5,6].

A critical aspect of the discussion is the balance between the protection of personal data and the need to use this information for the purposes of research and improving health services. The LGPD establishes legal bases that allow data to be processed for these purposes, as long as the appropriate security measures and privacy guarantees are adopted. This highlights the importance of an ethical and legally based approach to conducting health research, respecting the rights of individuals while seeking to advance scientific knowledge and improve the provision of health services[1,2].

The digitization of health services is viewed with optimism[11], who note significant progress in improving health services with the adoption of digital technologies, although they acknowledge the need for more robust data governance. Similarly, studies[12] warn of gaps in legislation regarding health impact assessments, highlighting the need for greater clarity. Similarly, Ramos et al.[10] explore the ethical and legal issues that arise with data protection in research and public administration. These findings suggest a consensus on the importance of data protection, but with a mixed perception of the current capacity of institutions to implement effective solutions, ranging from privacy concerns to confidence in technological advances.

A common theme identified in most studies is the urgent need to adapt health information systems to ensure compliance with the principles and requirements of the LGPD, especially with regard to data security and patients' informed consent[1-2,14-16].

The LGPD in Brazil represents a milestone in the protection of fundamental rights, establishing an important parallel with human rights[1], while highlighting the transformative role of digitalization in healthcare. This transformation, however, introduces challenges related to data security and the privacy of individuals[2], requiring a balance between technological innovation and the protection of personal data.

Anonymization appears to be a promising strategy to enable the safe use of data in research, indicating a potential way to circumvent some of the risks associated with the processing of personal data[11,15]. However, the legislation needs greater clarity as to the practical application of anonymization and specific guidelines for the processing of sensitive data[14,17], highlighting a critical aspect in the implementation of the LGPD in the health context.

One of the crucial points identified is the issue of consent, emphasized by the need to obtain explicit and informed consent from data subjects for the processing of health data[3-18]. This need poses particular challenges in clinical contexts, especially in emergencies or when consent can be an obstacle to accessing essential treatments.

For professionals, they highlight the need to protect data in sensitive contexts such as mental health, a practical and immediate challenge for health professionals[8]. On the other hand, researchers[6]

point to privacy risks in the broader context of digital health, emphasizing the need for ongoing training and awareness of data protection practices.

These different emphases reveal that the challenges of the LGPD are not uniform and vary according to the focus of the study and the specific health context in which they are inserted. For effective implementation, a balance is needed between systemic adjustments and professional training, ensuring that both are prepared to deal with the complexities of data protection in the digital age. Training healthcare professionals in the principles of the LGPD and data protection practices is fundamental[18-19], signaling a need for investment in training and awareness-raising to ensure compliance and security in the handling of patient data.

The effective implementation of the LGPD in the health sector requires a multi-faceted approach, involving not only technological and procedural adjustments, but also a commitment to the continuing education of health professionals. Such an approach is essential to navigating the challenges present at the intersection between data protection, technological innovation in healthcare, and the fundamental rights of individuals.

Conclusion

The implementation of the LGPD in the health sector, especially in telemedicine, presents both challenges and opportunities. Challenges such as the need to adapt health information systems, the implementation of informed consent, and the adoption of information security measures are highlighted. In addition, the lack of definition as to whether impact assessments are mandatory and the heightened need for data protection in mental health are specific challenges identified.

However, GDPR compliance also offers significant opportunities, such as increasing patient confidence in telehealth services and promoting innovation in data management practices. The cultural change required for full compliance with the LGPD, including ongoing education and training of healthcare professionals, is essential to ensure the security of patient data, promote privacy and drive innovation in digital health.

Continuing professional education is crucial to meeting the challenges posed by the LGPD. Investing in training healthcare professionals in data protection practices not only improves compliance with the legislation, but also strengthens patient trust and service efficiency. In addition, proper training enables professionals to better deal with the technical and ethical complexities involved in protecting health data. Other challenges for professionals include the need for constant updating in the face of technological and legal changes, the efficient management of informed consents and the adoption of innovative information security practices.

To successfully navigate this new legal and ethical landscape, it is essential that there is a joint effort between healthcare managers, IT professionals and legislators to develop strategies that not only meet legal requirements, but also promote continuous improvement in the quality and accessibility of healthcare.

Thanks

To Professor Cláudia Capelli and Tutor Thalles Fontainha for their encouragement and support.

Conflict of interest

The authors declare that there is no conflict of interest.

Authors' contribution

Lopes EKB contributed to the conception, design, analysis, writing, revision and approval of the final version of the article. Lopes FH contributed to the critical review of the article's content. Colonello NA contributed to writing the article and approving the final version. De Barros FPC contributed to writing the article and critically reviewing it. Avelar RS contributed to writing the article and critically reviewing its content.

References

1. De Aragão SM, Schiocchet T. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. Rev Eletron Comun Inf Inov Saúde [Internet]. 2020 [cited 18 Oct. 2024]; 14(3):692-708. Available from: https://www.reciis.icict.fiocruz.br/index.php/reciis/article/view/2012

2. Aith F. Saúde digital e os desafios regulatórios. R Dir Sanit [Internet]. 2021 [cited 18 Out. 2024]; 21:1-2. Available from: https://doi.org/10.11606/issn.2316-9044.rdisan.2021.193268

3. Brasil. Ministério da Saúde. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília: Ministério da Saúde [Internet]. 2024. [cited 18 Oct. 2024]. Available from: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd

4. Ursi ES. Prevenção de lesões de pele no perioperatório: revisão integrativa da literatura [dissertação]. Ribeirão Preto: Universidade de São Paulo, Escola de Enfermagem de Ribeirão Preto; 2005 [cited 18 Oct. 2024]. Available from: https://teses.usp.br/teses/disponiveis/22/22132/tde-18072005-095456/pt-br.php

5. Albuquerque A. Pesquisa com prontuário: análise ético-jurídica à luz dos direitos humanos dos pacientes. Cad ética pesqui [Internet]. 2019 [cited 18 Oct. 2024]; 1(1):41-52. Available from: https://pesquisa.bvsalud.org/portal/resource/pt/biblio-1281437

6. Leme RS, Blank M. Lei Geral de Proteção de Dados e segurança da informação na área da saúde. Cadernos Ibero-Americanos de Direito Sanitário [Internet]. 29 set. 2020 [cited 18 Oct. 2024]; 9(3):210-24. Available from: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/690

7. Almeida BDA, Doneda D, Ichihara MY, Barral-Netto M, Matta GC, Rabello ET, et al. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. Ciênc saúde coletiva [Internet]. Jun. 2020 [cited 18 Oct. 2024]; 25(suppl 1):2487-2492. Available from: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-81232020006702487&tlng=pt

8. Tietzmann AC, Heringer JI, Fernandes MS, Roberto GJ. Privacidade e confidencialidade das informações clínicas em saúde mental: velhos desafios em um novo contexto. Rev Bras Psicoter. [Internet]. 2021 [cited 18 Oct. 2024]; 23(3):165–75. Available from: https://pesquisa.bvsalud.org/portal/resource/pt/biblio-1355026

9. Camara MAA, Lins GHA, De Oliveira FHC, Camelo EMA, De Medeiros NRFC. Internet das Coisas e blockchain no Sistema Único de Saúde: a proteção dos dados sensíveis diante da Lei Geral de Proteção de Dados. Cadernos Ibero-Americanos de Direito Sanitário [Internet]. 18 mar. 2021 [cited 18 Oct. 2024]; 10(1):93-112. Available from: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/657

10. Ramos BEM, Madureira AS, Sena JP, Leal PST. Questões éticas e perspectiva jurídica da proteção de dados. Cadernos Ibero-Americanos de Direito Sanitário. [Internet]. 16 set. 2021 [cited 21 Oct. 2024]; 10(3):172-90. Available from: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/796

11. Pinto HA, Santana J SS, Chioro A. Por uma transformação digital que assegure o direito à saúde e à proteção de dados pessoais. Saúde em Redes [Internet]. 2022 [cited 6 Mar. 2024]; 8(2):361-371. Available from: http://revista.redeunida.org.br/ojs/index.php/rede-unida/article/view/3822

12. Vetis-Zaganelli M, Binda Filho DL. A Lei Geral de Proteção de Dados e suas implicações na saúde: as avaliações de impacto no tratamento de dados no âmbito clínico-hospitalari. Rev Bio y Der. [Internet]. 22 fev. 2022 [cited 18 Oct. 2024]; 215-32. Available from: https://revistes.ub.edu/index.php/RBD/article/view/36005

13. Almeida SCD, Soares TA. Os impactos da Lei Geral de Proteção de Dados - LGPD no cenário digital. Perspectivas em Ciência da Informação [Internet]. 1 set. 2022 [cited 18 Oct. 2024]; 27(3):26-45. Available from: https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/

14. Brasil. Ministério da Saúde. Portaria de Consolidação nº 2 de 28 de setembro de 2017. Brasília: Ministério da Saúde [Internet]. 2017 [cited 4 Jun. 2024]. Available from: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2017/prc0002_03_10_2017.html

15. Ministério da Saúde (Brasil). Comitê Gestor da Estratégia e-Saúde. Estratégia e-saúde para o Brasil. Brasília: Ministério da Saúde; 2017. Available from: https://pesquisa.bvsalud.org/portal/resource/pt/biblio-1348073?src=similardocs

16. Organização Mundial da Saúde. Global strategy on digital health 2020-2025. Geneva: World Health Organization; 2021 [cited 18 Oct. 2024]. Available from: https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf

17. Ministério da Saúde (Brasil). Secretaria Executiva. Departamento de Informática do SUS. Estratégia de Saúde Digital para o Brasil 2020-2028. Brasília: Ministério da Saúde; 2020. Available from: https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf

18. Brasil. Ministério da Saúde. Portaria nº 1.434 de 28 de maio de 2020. Institui o Programa Conecte SUS e altera a Portaria de Consolidação nº 1/GM/MS, de 28 de setembro de 2017, para instituir a Rede Nacional de Dados em Saúde e dispor sobre a adoção de padrões de interoperabilidade em saúde. Brasília: Ministério da Saúde [Internet]. 2020 [cited 4 Jun. 2024]. Available from: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2020/prt1434_01_06_2020_rep.html

19. Brasil. Ministério da Saúde. Portaria nº 1.768 de 30 de julho de 2021. Altera o Anexo XLII da Portaria de Consolidação GM/MS nº 2, de 28 de setembro de 2017, para dispor sobre a Política Nacional de Informação e Informática em Saúde (PNIIS). Brasília: Ministério da Saúde [Internet]. 2021 [cited 4 Jun. 2024]. Available from: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2021/prt1768_02_08_2021.html

How to cite

Lopes EKB, Lopes FH, Colonello NA, De Barros FPC, Avelar RS. Challenges in implementing the General Data Protection Law in telehealth services: an integrative review. Cadernos Ibero-Americanos de Direito Sanitário. 2025 jan./mar.;14(1):45-57
https://doi.org/10.17566/ciads.v14i1.1238