International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com || Volume 07 - Issue 06 || June 2022 || PP. 03-09

The reflections of the implementation of the general personal data protection law - LGPD in health plan operators

Solange Moretti[1], José Amarildo Avanci Júnior[2], Marcelo Fontes da Silva[3], Jéssica Carolina Garcia Avanci Moretti[4]

[1](*Faculty UNIMED, Brazil)*
[2](*Faculty of Medicine/ Federal University of Mato Grosso do Sul, Brazil)*
[3](*Faculty of Medicine/ Federal University of Mato Grosso do Sul, Brazil)*
[4](*Faculty of Medicine/ Federal University of Mato Grosso do Sul, Brazil)*

Abstract: With the evolution of technology, there was an uncontrollable interaction with the personal data of patients who have a relationship with health operators and, in this way, the need arose to reinforce the mechanisms of protection of this information, considering that society, in the current conjuncture, is based on technologies, which generates constant exposure. From the problem with privacy and security in the registration, storage and treatment of this data, the General Law for the Protection of Personal Data (LGPD) emerged to guarantee, mainly, their protection. In view of this perspective, the present study aimed to investigate how health operators are adapting to comply with the requirements of the LGPD regarding the personal and sensitive data of system users, as well as the adaptation and modification of the work routine of employees that guarantee the effectiveness and performance of the service provided. The study was of an applied nature, exploratory objective, quantitative approach and bibliographic procedure, being literature review research, consisting of scientific articles, case studies and news about the theme of the implementation of LGPD by operators of insurance plans. health. Scientific studies on such adjustments that health institutions must perform in the face of LGPD are still scarce, but several news and publications of data protection policies on the subject were found, indicating that the plans are seeking to adapt to the new reality that involves the privacy of patient and customer data.

Keywords: data protection; LGPD; personal data; sensitive data.

1. INTRODUCTION

When a patient seeks care at a health institution, it is necessary for him to provide various information and personal data, as well as his health plan and/or even his medical history. Such data can be attacked by criminals who seek to acquire them and thus enjoy undue advantages. With the evolution of technology that allowed the uncontrollable interaction with personal data, the need arose to strengthen the mechanisms of protection of personal data, given that society, in the current situation, is based on technologies, which generates constant exposure [1].

From the problem with privacy and security in the registration, storage and treatment of this patient data, the General Law for the Protection of Personal Data (LGPD) emerged to guarantee, mainly, the protection of this information [2]. Law 13,709 of 2018, LGPD, emerged to "protect the intimacy, privacy of citizens and their rights, where in modern times this defense gains strength in respect of democracy and the right of the individual to protect his personality"; bringing relevance to the idea of correct and organized use of the internet by both citizens and organizations, for example as seen in health plan operators; rather, without due precaution with the protection of these data that are transmitted via the internet, demonstrating the need for companies to adjust to the new law [3].

Personal information has always been very vulnerable to cyber-attacks since the beginning of the digital age, especially in today's increasingly online society, especially when referring to social networks and in organizational records. Limiting access to this data by third parties often depended on the user, having considerable influence of the social network organization in maintaining the security of the holder of such information [4].

The right to health information, personal data protection and governance is everyone's right and the different ways of defining privacy throughout history indicate that this notion is not unanimous and the type of protection is based on the different uses and purposes of the collection, treatment and nature of the information that is intended to be produced. The right to information is now emphasized as the right to control the use that others make of personal information, constituting the right to information [5].

According to the LGPD, the treatment of patient data refers to any operation performed with them, such as collection, processing, transmission, modification and storage. Such data (name, RG, CPF, biometric data, as

well as routes taken daily, name of parents) may, from now on, be used only with the explicit consent of the user, who must be informed about the type of operation to be that your data are submitted and if they will be shared, with the possibility of revoking such consent [6].

In view of this law sanctioned in 2018 and enacted in 2020, institutions will need to adapt their systems and their employees, in order to create "internal regulatory policies so that they can pass on greater confidence and transparency in the use of information to their users, if this is not the case." happens, sanctions imposed by law will be applied" [7].

Different types of data should be the object of attention of health operators according to these new dynamics imposed by the LGPD, highlighting the treatment of the most sensitive personal data that involve very intimate and individual issues (racial, ethnic, ideological and of sexual orientation, in addition to confidential information regarding the individual's health) which, depending on improper availability, can be used as an instrument of discrimination, intolerance and embarrassment [8].

Information security is based on the concepts of confidentiality and this is treated as a guarantee that access to information is restricted to its legitimate users. From the moment the data is entered into the operator's database, the confidentiality process begins and it is the operator's responsibility to protect it against undue, intentional or accidental changes [9].

The human factor is the main challenge for the implementation of good information security practices in the company, observing the need to implement new procedures regulated by law for the treatment and storage of information always with the objective of protection [10].

In view of this perspective, the present project aimed to investigate how health operators in Brazil are adapting to comply with the requirements of the LGPD regarding sensitive personal data of users of the system, as well as the adaptation and modification of the work routine of employees that guarantee the effectiveness and performance of the service provided.

2. MATERIAL AND METHODS

The study was of an applied nature, exploratory objective, quantitative approach and bibliographic procedure, being a work of literature review, consisting of scientific articles, case studies and news on the theme of the implications of the implementation of the General Protection Law of Personal Data – LGPD by health plan operators in Brazil.

For this, the Virtual Health Library (VHL) will be used as a research source through the following databases: PubMed, U.S. National Library of Medicine (NLM), Medline (Online System of Search and Analysis of Medical Literature), Lilacs (Latin American and Caribbean Literature in Health Sciences), SciELO (Scientific Electronic Library Online) and Google Scholar.

The inclusion criteria were studies and reports or news found in the period from 2018 to 2022, which addressed the methods of implementing the LGPD by Brazilian health plan operators, as well as the appropriate adjustments. All studies that did not meet the inclusion criteria were excluded.

3. RESULTS AND DISCUSSION

When comparing the sectors that deal with people's sensitive data, health is one of the main responsible for the manipulation of these and the violation of this information can be harmful to the individual. The health sector is one of the sectors that most process data considered sensitive and whose violation can cause serious damage to the individual. According to the Federal Data Processing Service, SERPRO, sensitive data "are those that reveal racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, genetics, biometrics and about a person's health or sex life" [11].

The data processing limit applied to the health sector is a fundamental theme in the LGPD and, in a special way, for the market of health plan operators, since it deals with the principle of non-discrimination. It is worth noting that communication or shared use between controllers of sensitive personal data relating to health for the purpose of obtaining economic advantageis prohibited [12].

Some private institutions use the LGPD to develop their own policies, such as the Privacy and Data Protection Policy of the company UNIMED Campo Belo [13]. The policy implemented by the institution requires the consent of the "Personal Data Subject" available on the Corporate Portal, or for the effective use of any Portal, system, software, application or service of this branch. To this end, the company provides employees with terms that facilitate the transition of systems in accordance with the LGPD (figure 1).

Figure 1: Terms that help employees of a private company in the transition of systems according to LGPD.

Dado pessoal	Informação relacionada à pessoa natural, direta ou indiretamente, identificada ou identificável.
Dado pessoal sensível	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
Banco de dados	Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
Titular	Pessoa natural a quem se referem os dados pessoais, tais como antigos, presentes ou potenciais clientes, colaboradores, contratados, parceiros comerciais e terceiros.
Controlador	Pessoa natural ou jurídica, de direito público ou privado, a quem competem às decisões referentes ao tratamento de dados pessoais.
Anonimização	Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
Consentimento	Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
Compartilhamento	Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.
Relatório de impacto à proteção de dados pessoais (RIPD)	Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
Autoridade Nacional de Proteção de Dados (ANPD)	Órgão responsável por zelar, implementar e fiscalizar o cumprimento da legislação de proteção de dados pessoais.

Source: UNIMED, 2021a.

The company UNIMED SÃO SEBASTIÃO DO PARAÍSO also underwent a process of readjustment after the publication of the LGPD, which indicates that it strictly respects the principle of legality for the treatment of its customers' personal data, being possible to do so only in the context of in any of the legal bases provided for in the Brazilian legislation for the protection of personal data, with the consent of the holder, to comply with a legal or regulatory obligation, for the execution or preparation of a contract, for the exercise of rights in judicial, administrative or arbitration proceedings, for the protection of the life or physical safety of the holder or third parties [14].

Regarding the adaptation of health providers with the LGPD, authors bring that “both health plan operators and service providers are responsible for the information they have from third parties and for decisions regarding the processing of personal data” and thus all the rules that must guarantee the confidentiality of the data of the that were already running before the LGPD should continue to be applied, but now complemented by the new legislation [15].

For the National Association of Private Hospitals [16], the use of information and communication technology resources in the health area is increasing, where data travel in large volumes (and not always in an orderly manner), being applied to resources such as medical records. patient electronics (PEP), telemedicine, information exchange between institutions and in the care area, among others. Consequently, the standardization and adequate regulation of the use of such information is necessary, according to the LGPD, according to its specificities.

The LGPD also cites anonymized data, which is data that originally related to a person, but which lost the possibility of association, directly or indirectly, with an individual, considering the reasonable technical means available at the time of treatment. In this case, the LGPD will not apply to it and so the company will not need to adapt to these peculiarities. The personal data collected are used to improve or create new products and services for customers and main audiences, to enable the provision of care services to other cooperatives and

auxiliary companies to comply with legal or regulatory obligations, to carry out research related to its activities - with the consent of the holder without prejudice to the interests, rights and fundamental freedoms of the holder [17].

Institutions must ensure that all personal data processing activities comply with the 10 (ten) principles brought by the legislation on privacy and data protection (figure 2).

Figure 2: Principles under the LGPD.

PRINCÍPIO	APLICAÇÃO PRÁTICA
Finalidade	Um dado que foi coletado para uma finalidade, não pode ser posteriormente utilizado para outra.
Adequação	O tratamento e as atividades relacionadas ao tratamento devem condizer com as finalidades declaradas.
Necessidade	Além de cumprir a lei, quem trata dados pessoais também terá que comprovar que cumpre com as obrigações da LGPD.
Livre acesso	Os dados tratados devem ser acessíveis pelos titulares.
Qualidade dos dados	Os dados devem ser mantidos atualizados e completos, para não prejudicar o titular.
Transparência	Os titulares devem ser informados de todos os detalhes sobre o tratamento de seus dados, e devem ser capazes de facilmente acessar esta informação.
Segurança	Devem ser adotadas medidas para proteger os dados pessoais de incidentes de segurança.
Prevenção	Não utilizar dados pessoais de formas que prejudiquem o titular, ou que o discriminem injustamente.
Não discriminação	Além da segurança, devemos evitar que dados pessoais sejam expostos desnecessariamente.
Responsabilização e prestação de contas	Somente deverão ser tratados os dados que realmente são necessários para atingir a finalidade

Source: UNIMED, 2021b.

For a treatment activity promoted by health plans to be considered legitimate and adequate to the LGPD, it must be accommodated in one of the hypotheses as shown in Figure 3.

Figure 3: Treatments and hypotheses according to LGPD.

BASE LEGAL	APLICA-SE	REQUISITOS
Consentimento do titular	Quando nenhuma outra base legal puder justificar o tratamento, o titular precisa dar seu consentimento	O consentimento deve ser específico, livre, informado, e deve ser revogável
Obrigação legal ou regulatória	Quando uma norma, lei, regulamento ou decisão judicial obriga o tratamento dos dados pessoais	O tratamento deve ser uma obrigação (Não pode ser opcional)
Pela administração pública	Para a execução de políticas públicas	Somente pode ser usada por órgãos da administração pública
Estudos por órgão de pesquisa	Realização de pesquisas e estudos	Somente pode ser usada por órgãos de pesquisa (Sem fins lucrativos)
Contrato com o titular	Quando o tratamento é necessário para o cumprimento de contrato com o titular, ou para possibilitar o cumprimento futuro	O tratamento deve ser indispensável para o cumprimento do contrato, que deve ser firmado com o titular
Exercício regular de direito	Quando o tratamento é necessário para a defesa de direitos em processos administrativos, judiciais ou arbitrais	Os dados devem ser necessários para utilização em processo administrativo, judicial ou arbitral
Proteção da vida	Em situações de vida ou morte, ou para proteger a incolumidade física do titular ou de terceiro	A vida ou incolumidade física de alguém deve estar em risco para justificar o enquadramento
Tutela da saúde	Para a realização de procedimentos visando a proteção da saúde do titular	Somente pode ser usada por profissionais de saúde, autoridade sanitária, ou serviços de saúde
Legítimo interesse	Para apoiar as atividades do controlador, ou para o benefício do titular	Estar alinhado com as expectativas do titular, respeitados os seus direitos
Proteção do crédito	Quando o tratamento tiver como finalidade a proteção de crédito	Deve respeitar a legislação aplicável à proteção de crédito (Exemplo: Lei nº 12.414/11)
Segurança ou prevenção à fraude	Quando a informação sensível é utilizada para garantir a segurança do titular ou prevenir fraudes, nos processos de identificação e autenticação de cadastro	O titular deve estar ciente da forma em que seus dados sensíveis são utilizados

Source: UNIMED, 2021b.

The company SAÚDE CONCEIÇÃO [18] brings to its employees the main personal data of holders that may be processed by the Operator in the exercise of its functions and its main purpose. This list serves as a reference and guidance and is not intended to relate all data and their purposes (figure 4).

Figure 4: Main personal data of holders that may be processed by the Operator.

CATEGORIAS DE DADO	FINALIDADES
Dados de identificação pessoal: Nome, endereço residencial, endereço de correspondência, filiação, data de nascimento, telefone residencial, telefone celular, e endereço de e-mail, cartão nacional de saúde, carteira civil, CNH, CPF, CRM, inscrição no INSS, matrícula funcional, PIS/PASEP, placa do automóvel.	Contratação de planos de saúde por parte de clientes; Contratação de colaboradores; Registro de visitantes; Utilização de instalações físicas; Ações de marketing e comunicação diretas ao cliente.
Dados pessoais e curriculares contendo histórico profissional, registro de absenteísmo, históricos acadêmicos e dados de contato enviados através de email, processos disciplinares de RH.	Processos seletivos para colaboradores; Administração de recursos humanos.
Biometria digital, fotografia da face dos colaboradores, imagens de colaboradores e visitantes em áreas de circulação.	Registro de ponto, envio de emails com foto na assinatura, monitoramento e vigilância de áreas físicas e patrimônio da empresa.
Dados bancários (banco, agência e conta), histórico de pagamentos, cartão de crédito, histórico de procedimentos realizados, informações de bureau de crédito.	Processamento financeiro de pagamento e cobrança de serviços realizados.
Informações de pesquisas de opinião.	Avaliar a satisfação dos trabalhos realizados.

Source: SAÚDE CONCEIÇÃO, 2021.

According to the guidelines established by the company NossaSaúde[19], personal information from patients is only requested when "we really need it to provide a service", doing so by fair and legal means, with the knowledge and consent of the same. The company has also adapted in terms of informing why it is being collected and how it will be used, in addition to storing the data and protecting it from unauthorized access, disclosure, use or modification.

According to UNIMED BRASIL [20] personal data from the LGPD are used to improve or create new products and services for customers and main audiences, to enable the provision of care services with other cooperatives and auxiliary companies of the Unimed System, for the fulfillment of a legal or regulatory obligation, for carrying out research related to its activities - with the consent of the holder - or for the legitimate interest of the company, without prejudice to the interests, rights and fundamental freedoms of the holder.

Unimed Blumenau [21] underwent an Adaptation Project to the LGPD. Lasting 12 months, this project had several stages:

- *Constitution of a Privacy Governance Committee;*
- *Evaluation and Training of the Board, Managers, Coordinators/Leaders and Committee;*
- *Hiring the Person in Charge for Data Processing;*
- *Mapping of Personal Data;*
- *Assessment of Risks related to Data Protection, with the preparation of action plans to mitigate and prevent risks;*
- *Creation of the Data Protection Policy;*
- *Document Compliance aiming at the protection of personal data;*
- *Creation of criteria for monitoring and constant updating of the privacy governance program.*

According to São Pietro Saúde[22], its website was also adapted to comply with the rules set out in the LGPD, with the following principles:
– The user's personal data will be processed in a lawful, fair and transparent manner;
– The user's personal data will only be collected for specific, explicit and legitimate purposes (limitation of purposes);
– The user's personal data will be collected in an appropriate, relevant and limited way to the needs of the purpose for which they are processed;
– The user's personal data will be accurate and updated whenever necessary, so that inaccurate data are deleted or rectified when possible;
– The user's personal data will be treated securely, protected from unauthorized or unlawful treatment and against accidental loss, destruction or damage, adopting the appropriate technical or organizational measures (integrity and confidentiality).

For the ATHENA SAÚDE (2020) group, its policy of adaptation to the LGPD applies to the processing of personal data of beneficiaries and dependents as well as users of operator websites and applications. The ATHENA group goes against most health institutions, where its recommendation is that if the individual is an

employee, collaborator or supplier, the person should seek the respective privacy policy to obtain the applicable terms and inform him about his rights to your data; while the other operators spontaneously inform their guidelines and mandatorily apply their adaptation policy to the new Law for all situations involving customer data.

4. FINAL CONSIDERATIONS

As of August 16, 2020, the General Data Protection Law (LGPD) began to regulate the use, protection and transfer of personal data in Brazil. This new law is demanding a series of changes in the data security policy of healthcare operators. The main one is that beneficiaries become holders of their data and have full rights over all health information collected about them.

The entry into force of the LGPD should profoundly change the way in which information technology in supplementary health is worked, however, what is observed through research is that not all operators have adapted to the new reality, on the other hand, many are already seeking such adaptations.

Results such as the one presented in this study demonstrate the importance of turning attention and perspectives to current and so necessary content such as those involving data from clients of large health institutions. In this way, it is expected to create subsidies and incentives for new research on updates from health operators regarding the protection of patient data.

REFERENCES

[1] M.R. De Flôres. Desafios e perspectivas da proteção de dadospessoaissensíveisempoder da administraçãopública: entre o deverpúblico deinformareodireitodocidadãodesertutelado.RevistadeDireito, vol.12, n.2, 2020.

[2] L.ALMEIDA.LGPDnasaúde:tudoquevocêprecisasabersobreanovalei.Disponívelem:http://blog.medcloud.com.br/lgpd-na-saude-tudo-que-voce-precisa-saber-sobre-nova-lei/.Acessoem: 20 dez.2021.

[3] M.V.M.RIBEIRO. Nossosdadosnaera digital: Lei Geralde Proteçãode Dados. Revista Conhecimento Interativo, vol.14, n.2, p.362-382, 2020.

[4] F.P. PIURCOSKY*et al*. A lei geral de proteção de dados pessoaisemempresasbrasileiras: umaanálisedemúltiploscasos. Suma deNegócios,vol.10, n.23, 2019.

[5] M. VENTURA.Paraalémdaprivacidade: direitoàinformaçãonasaúde, proteção de dados pessoais e governança. Cadernos de SaúdePública, vol. 34, n.7,2018.

[6] R. VELHO. Em vigor a partir de agosto, implementação da Lei Geral de Proteção de Dadosaindaenfrentadesafios. Ciênciae Cultura, vol.72,n.2, 2020.

[7] M. V. M. RIBEIRO. Nossosdadosnaeradigital: Lei Geralde Proteçãode Dados. Revista Conhecimento Interativo, vol.14, n.2, p.362-382, 2020.

[8] M.R. De Flôres. Desafios e perspectivas da proteção de dadospessoaissensíveisempoder da administraçãopública: entre o deverpúblico deinformareodireitodocidadãodesertutelado. Revistade Direito, vol.12, n.2, 2020.

[9] F.P. PIURCOSKY *et al*. A lei geral de proteção de dados pessoaisemempresasbrasileiras: umaanálisedemúltiploscasos. Suma deNegócios,vol.10,n.23,2019.

[10] I. GHAFIR, *et al*. Security threats to critical infrastructure: the human factor. Journal of Super computing,vol, *74, n.*10, p.4986-5002,2018.

[11] E. SALES. Descomplicando a LGPD: Conheçaosprincipaisconceitosemtorno do tema. Animus. 2022. Disponívelem: animuscj.com.br/post/descomplicando-a-lgpd. Acessoem: 15 jun. 2022.

[12] J.M.DA COSTA. Lei geral de proteção de dados aplicada à saúde. Revista Humanidades e Inovação, v. 8, n. 45, 2021.

[13] UNIMED CAMPO BELO. Politica de privacidade e proteção de dados. 2020b. Disponívelem: https://www.unimedribeirao.com.br/politica-de-privacidade-e-protecao-de-dados. Acessoem: 15 jun. 2022.

[14] UNIMED SÃO SEBASTIÃO DO PARAÍSO. Politica de privacidade e proteção de dados da UNIMED SÃO SEBASTIÃO DO PARAÍSO. 2021a. Disponívelem: unimed.coop.br/documents/1250554/2329571/Politica+de+Privacidade/a2a3918e-015a-40a7-bff4-

2fcd1d48f8b8. Acessoem: 15 jun. 2022.

[15] L.O.HAWRYLISZYN. Lei geral de proteção de dados (LGPD): o desafio de suaimplantação para a saúde. RevistaUnivap, v. 27, n. 54, 2021.

[16] ASSOCIAÇÃO NACIONAL DE HOSPITAIS PRIVADOS - ANAHP. Lei Geral de Proteção de Dados: RecomendaçõesAnahp para oshospitais. São Paulo: ANAHP, 2019. Disponívelem: https://conteudo.anahp.com.br/cartilha-lgpd-anahp. Acessoem: 15 jun. 2022.

[17] UNIMED. Política de Privacidade. 2022. Disponívelem: unimed.coop.br/site/politica-de-privacidade. Acessoem: 15 jun. 2022.

[18] SAÚDE CONCEIÇÃO. Políticas de Privacidade e Termos de Uso. 2021. Disponívelem: https://planodesaudeconceicao.com.br/politicas-de-privacidade-e-termos-de-uso/. Acessoem: 15 jun. 2022.

[19] NOSSA SAÚDE OPERADORA DE PLANO DE SAÚDE. Política de privacidade e proteção de dados. 2022. Disponívelem: nossasaude.com.br/politica-de-privacidade/#:~:text=Os%20dados%20pessoais%20tratados%20pela,exemplo%2C%20a%20guarda%20de%20prontuários. Acessoem: 15 jun. 2022.

[20] UNIMED CAMPO BELO. Politica de privacidade e proteção de dados. 2020b. Disponívelem: https://www.unimedribeirao.com.br/politica-de-privacidade-e-protecao-de-dados. Acessoem: 15 jun. 2022.

[21] UNIMED BLUMENAU. Proteção de dados. 2022. Disponívelem: https://www.unimed.coop.br/site/web/blumenau/lgpd. Acessoem: 15 jun. 2022.

[22] SÃO PIETRO SAÚDE. Política de Privacidade. 2021. Disponívelem: https://saopietro.com.br/politica-de-privacidade/. Acessoem 15 jun. 2022.

[23] ATHENA SAÚDE. Política de privacidade e proteção de dados. 2020. Disponívelem: https://www2.samp.com.br/data/files/7F/91/6D/48/0A58971020CE5F776A4AF9C2/LGPD_PL004_POLITICA%20DE%20PRIVACIDADE%20E%20PROTECAO%20DE%20DADOS%20OPERADORAS%20DE%20SAUDE%20_1_.pdf. Acessoem: 15 jun. 2022.