ARQUIVOS DE ASMA, ALERGIA E IMUNOLOGIA




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

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

**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]**

**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.

**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.

## Introdução

Você possui uma clínica médica e lida com dados pessoais de vários pacientes, todos os dias. Estes dados são necessários para prestar o atendimento e, por vezes, revelam informações sigilosas sobre as condições de saúde dos pacientes. Em 2018, foi publicada uma Lei que regulamenta o tratamento de dados pessoais em todos os setores da economia: a Lei Geral de Proteção de Dados (LGPD)[1]. Apesar de publicada

1. Coordenador da Comissão de Estatuto, Regulamentos e Normas (gestão 023/2024), da Associação Brasileira de Alergia e Imunologia (ASBAI).
2. Membro da Comissão de Estatuto, Regulamentos e Normas da ASBAI – gestão 2023/2024.
3. Presidente da ASBAI – gestão 2023/2024.
4. Diretor de Pesquisa da ASBAI – gestão 2023/2024.
5. Advogado, Mestre em Direito Digital pela Universidade Federal de Minas Gerais (UFMG). Professor de Graduação e de Pós-Graduação em Proteção de Dados e Direito Digital - Pontifícia Universidade Católica de Minas Gerais (PUC Minas) e CEDIN.
6. Advogada, Mestre em Direito pela UFMG. Técnica em Informática, com ênfase em programação de computadores - CEFET-MG.
7. Advogado. Mestrando em Direito e Tecnologia pela UFMG. Pós-Graduado em Direito Digital - PUC Minas.

Submetido em: 21/04/2024, aceito em: 02/11/2024.

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

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

em 2018, a LGPD só entrou em vigência completa em agosto de 2021. Ao longo destes quase quatro anos, ficou suspensa a possibilidade de aplicação de sanções administrativas, visando que os agentes de tratamento se adequassem à Lei e possibilitando a estruturação da Autoridade Nacional de Proteção de Dados (ANPD), autoridade fiscalizadora da lei. De lá para cá, a ANPD recebeu diversas denúncias e reclamações e instaurou processos administrativos, sancionadores e inclusive aplicou sua primeira multa por descumprimento da LGPD em 2023.

A LGPD determina como os dados pessoais deverão ser cuidados e possui interface com outras normas, como o Código de Ética Médica. Por isso, deve ser objeto de estudo por todos que possuem contato com dados pessoais, independentemente do volume de dados ou do porte da clínica.

Nesse artigo serão abordados os principais cuidados a serem tomados na utilização dos dados dos pacientes, compreendendo conceitos fundamentais da LGPD e o contexto de digitalização dos serviços de saúde. Também serão apresentados cuidados importantes sobre as responsabilidades a que os médicos estão sujeitos no tratamento dos dados, seja na esfera administrativa, seja na esfera cível.

## Conceitos básicos

### *O que é um dado pessoal?*

Dado pessoal é toda informação relacionada à pessoa natural identificada ou identificável. Ou seja, o dado precisa ser de uma pessoa física e deve ou identificar diretamente uma pessoa, ou ter o potencial de identificá-la.

Um exemplo do primeiro caso é o cadastro de pessoa física (CPF), trata-se de dado que identifica diretamente seu titular. No segundo caso, é preciso analisar se o conjunto de informações permite identificar alguém. Por exemplo, na brincadeira do amigo oculto, à medida em que características de uma pessoa são apresentadas, ela vai se tornando identificável. Ou seja, mesmo informações triviais como cor do cabelo, altura e a vestimenta possuem o condão de identificar alguém, em determinado contexto.

Assim, as informações de saúde de alguém podem identificá-la, seja porque tem uma doença rara, seja porque é uma pessoa pública cujas características de saúde são evidentes.

A LGPD ainda traz uma categoria específica de dados pessoais, que são especialmente protegidos: os dados pessoais sensíveis.

Esses dados são aqueles que podem causar algum tipo de discriminação ao titular, como, por exemplo, dados referentes à origem racial, étnica, convicção religiosa, opinião política, e dados de saúde. Esses dados somente podem ser utilizados de maneiras restritas e, por isso, é preciso um cuidado a mais ao tratá-los. Por exemplo, não é possível compartilhar estes dados com outras pessoas para obter vantagens econômicas, salvo se o compartilhamento for necessário para a prestação dos serviços. Assim, um Hospital pode compartilhar os dados de saúde com Operadoras de Saúde, mas não pode vendê-los, por exemplo, para a indústria farmacêutica.

Atenção: muitas pessoas acreditam que dados como CPF, balanços financeiros e dados bancários são dados pessoais sensíveis, mas isto não é verdade. Embora sejam informações importantes, não são classificados pela LGPD como dados pessoais sensíveis. Saber a diferença é essencial, pois isso é necessário para definir a base legal adequada para cada operação de tratamento de dados – e elas variam conforme esteja-se diante de dados comuns ou sensíveis. Se você não sabe o que é uma base legal, não se preocupe. Falaremos sobre ela e porque ela é importante nos próximos tópicos.

### *Tratamento de dados pessoais*

A LGPD se aplica a todas as atividades do que chama de “tratamento de dados pessoais”. Por isso, além de saber o que são dados pessoais, é necessário identificar o conceito de tratamento. A LGPD detalhou diversos verbos para definir o que é tratamento de dados pessoais. Os termos utilizados pela Lei são os seguintes: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Na prática, tudo que se faça com um dado pessoal se enquadra no conceito. Seja recebendo os dados, armazenando, enviando, ou processando, você sempre estará, nas rotinas de atendimento, tratando dados pessoais. Esses exemplos são espécies do gênero tratamento de dados, que engloba todas as ações possíveis.

Mesmo que você receba uma ficha de atendimento física e a armazene em sua gaveta, você fará uma atividade de tratamento de dados pessoais, considerando que a LGPD se aplica tanto aos dados digitais

quanto àqueles que trafegam de forma física. Assim, para cada atividade de tratamento, é preciso definir a base legal mais adequada.

### *O que são bases legais?*

Bases legais são os fundamentos jurídicos que uma atividade de tratamento de dados deve ter para que esteja em conformidade com a LGPD. Somente se o uso do dado tiver uma base legal, ele poderá ser feito, daí sua importância.

A LGPD permite o tratamento de dados em inúmeras hipóteses: existem 10 possíveis bases legais para o tratamento de dados comuns e oito respaldando o tratamento de dados pessoais sensíveis, conforme demonstrado na Tabela 1.

A mais famosa delas é o consentimento, que significa uma manifestação de vontade inequívoca do titular pela qual ele autoriza a utilização desses dados. Embora essa base legal seja a mais famosa, ela não é necessariamente a mais adequada para todos os casos – muitas vezes, inclusive, evitá-la é mais interessante na prática. Por exemplo, você provavelmente já sabe que precisa armazenar o prontuário[2,3] do paciente, por, no mínimo, 20 anos, no caso de documentos impressos em papel (a Lei 13.787/2018 permite a exclusão dos prontuários em papel ou digitalizados após 20 anos; já a Resolução CFM nº 1.821/2007, estabelece um prazo diverso ao determinar que para os prontuários digitalizados ou microfilmados, esse armazenamento deve ser per-

**Tabela 1**
Bases legais para dados comuns e dados sensíveis

| Dados comuns | Dados sensíveis |
|---|---|
| Consentimento | Consentimento |
| Cumprimento de obrigação legal ou regulatória | Cumprimento de obrigação legal ou regulatória |
| Execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumento congêneres | Execução de políticas públicas previstas em leis e regulamentos |
| Realização de estudos por órgão de pesquisa | Realização de estudos por órgão de pesquisa |
| Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados | – |
| Exercício regular de direitos em processo judicial, administrativo ou arbitral | Exercício regular de direitos, inclusive em contrato, em processo judicial, administrativo ou arbitral |
| Proteção da vida ou da incolumidade física do titular ou de terceiro | Proteção da vida ou da incolumidade física do titular ou de terceiro |
| Tutela da saúde | Tutela da saúde |
| Legítimos interesses do controlador ou de terceiros | – |
| Proteção ao crédito | Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos |

manente. Assim, caberá ao encarregado a análise da regulação aplicável ao caso para determinar o tempo de guarda do documento).

Portanto, para as hipóteses de armazenamento dos prontuários, o consentimento não é uma base legal adequada, pois mesmo que o paciente não concorde com o armazenamento, ainda assim ele será feito (ou seja, não se trata de caso em que o consentimento do titular é de fato relevante). Para estes casos, a base legal seria o "cumprimento de obrigação legal ou regulatória". Outra base legal bastante utilizada na área médica é a de "execução do contrato". Muitas vezes você precisa utilizar informações do paciente para cumprir com o próprio contrato firmado com você ou com o Plano de Saúde a partir do qual o atendimento é prestado.

Ainda, você pode utilizar os dados do prontuário do paciente para se defender em processos judiciais, nos casos, por exemplo, de alegação de erro médico. O Código de Ética Médica[4] autoriza a quebra do sigilo médico em caso de justo motivo ou de autorização prévia do paciente (artigos 73 e 89 do Código de Ética). A LGPD, por sua vez, reconhece que informações sensíveis podem ser utilizadas em ações judiciais para o exercício de direitos em processos nos quais a pessoa sobre a qual os dados versam seja parte. Ou seja, há respaldo legal para o uso do prontuário em processo, mas devem ser observadas diversas regras para tanto.

Uma base legal também bastante utilizada nos ambientes médicos é a "tutela da saúde". Ela costuma ser a hipótese mais adequada para os procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridades sanitárias. Para adotar essa base legal, contudo, é necessário que o tratamento de dados seja feito por profissionais de saúde, ou seja, pessoas que estejam sujeitas ao dever de sigilo estabelecidos pelos respectivos Conselhos Profissionais, tais como o Conselho Federal de Medicina, Conselho Federal de Farmácia, Conselho Federal de Enfermagem, dentre outros.

Outra base legal relevante é o legítimo interesse. Ela pode ser adotada, por exemplo, para atividades de apoio e promoção das atividades da sua clínica. Você pode, em alguns casos e tomados os cuidados necessários, utilizar os e-mails dos seus pacientes para enviar comunicações e notícias relevantes. Vale dizer, contudo, que essa base legal não é apta a justificar o tratamento de dados sensíveis. Você não pode usar os dados do prontuário do paciente (dados de saúde) para atingir uma finalidade de interesse da sua clínica ou de algum parceiro.

Por fim, vale saber que, no caso de dados de crianças e adolescentes, a LGPD traz sistemática própria, com grau ainda maior de proteção. As bases legais nesses casos são mais restritas e deve sempre ser observado o melhor interesse da criança ou do adolescente.

A avaliação das bases legais é complexa, e deve ser feita por um especialista. Muito mais do que definir qual base legal é compatível com cada atividade, esse profissional deve ser capaz de organizar toda a sua infraestrutura para estar em conformidade com a legislação.

## Responsabilidades do médico

O não cumprimento da LGPD pode resultar em penalidades financeiras significativas para os médicos, além de danos à reputação e confiança dos pacientes. Portanto, a conformidade com a lei é essencial para evitar essas consequências negativas. Vale aprofundamento sobre essas responsabilidades.

### *Responsabilidade administrativa*

A primeira espécie de responsabilidade com base na LGPD é a administrativa, ou seja, aquela que deriva do não cumprimento da lei e cuja fiscalização compete à ANPD. O descumprimento da LGPD sujeita os consultórios e clínicas a sanções que variam de advertência a uma multa de até 2% (dois por cento) do seu faturamento no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração[5].

Embora uma multa possa ser assustadora, é importante ter em mente que outras penalidades podem ser aplicadas, por exemplo, a suspensão parcial ou total do exercício de atividades relacionadas a tratamento de dados. Se isso ocorrer, você estará proibido de tratar dados, o que, na prática, pode significar o fim das suas atividades. Ainda, a reputação da sua clínica pode ser prejudicada, mesmo que, posteriormente, a sanção seja revertida.

Outra responsabilidade administrativa que, embora não esteja diretamente ligada à proteção de dados, pode ser acionada, é aquela perante os conselhos profissionais, como o Conselho Federal de Medicina e o Conselho Regional de Medicina. Já há notícia de condenações nesse sentido, perante o Conselho

Regional de Medicina do Ceará (CREMEC)[6], em que o médico exibiu casos clínicos identificáveis, com imagens de pacientes em anúncios profissionais.

O tratamento de dados pessoais irregular levou a uma sanção administrativa, com a cassação do registro do profissional.

### *Responsabilidade judicial*

O médico também pode ser considerado responsável na esfera judicial. Aqui, estamos diante da responsabilidade civil, aplicável nos casos em que, por ação ou omissão, negligência ou imprudência, alguém causa danos a outra pessoa. Nesses casos, nasce o dever de reparar os danos causados, que podem ser morais ou materiais.

A extensão dessa responsabilidade será verificada pelo juiz caso o paciente se sinta lesado. No caso da proteção de dados, esse tipo de ação pode existir se houver um vazamento de dados que leve à exposição indevida dos dados sensíveis de um paciente. Se, em função desse vazamento, houver danos à honra do paciente, ou se, em função dele, houver discriminação, poderá ser configurada a responsabilidade do médico.

O valor desse tipo de condenação é difícil de quantificar. No caso de incidentes envolvendo instituições financeiras, por exemplo, o Tribunal de Justiça de Minas Gerais tem aplicado condenações por danos morais em uma média de R$ 8.000,00 (oito mil reais)[7]. Ainda que o contexto dessas condenações já mapeadas seja distinto de casos de responsabilização de médicos, vale ter em mente que os valores podem ser de norte pelos juízes, em se tratando de danos por violação à LGPD.

Além dos danos morais eventualmente cabíveis, se o paciente demonstrar que teve prejuízos financeiros, podem também ser quantificados danos materiais em função do tratamento irregular.

### *Responsabilidade contratual*

Uma última responsabilização diz respeito às cláusulas contratuais. Se você atende Planos de Saúde, provavelmente firmou com a Operadora um contrato de credenciamento, pelo qual as responsabilidades com relação ao tratamento dos dados estão definidas. Se possui um contrato particular, essas responsabilidades também podem estar definidas, com previsão de penalidade em caso de descumprimento.

De toda forma, o dever de guarda e de segurança com relação aos dados do paciente é obrigação legal, e a falha em cumpri-los pode ser considerada uma quebra contratual. Assim, as multas e penalidades dispostas no contrato poderão ser acionadas pela parte que se sentir lesada.

## Diante dos cenários de riscos e incertezas, o que fazer? É o que se passa a analisar. Como estar em conformidade com a LGPD?

Buscar a conformidade com a LGPD em consultórios médicos é uma tarefa multidisciplinar que requer a colaboração de diferentes profissionais e áreas de especialização. Deve-se buscar a proteção adequada aos dados dos pacientes.

Desde já, um alerta importante: não é possível estar em conformidade com a LGPD apenas por um trabalho pontual, como, por exemplo, publicando uma política de privacidade no site da clínica.

Como o tratamento de dados é contínuo e diário, o processo de adequação à LGPD também o será. Por essa razão, o melhor jeito de você se adequar à Lei é estabelecendo um Programa de Governança em Proteção de Dados permanente. O programa deverá ser gerido por um encarregado pelo tratamento dos dados pessoais (ou DPO – *Data Protection Officer*), que pode ser uma pessoa física (indivíduo) ou jurídica (empresa ou escritório), e terá como característica o monitoramento constante das suas atividades.

Mais do que simplesmente elaborar uma série de documentos padrão, o DPO deve ser capaz de identificar a legislação aplicável, bem como as constantes alterações, garantindo que você esteja em conformidade com a lei e consiga aproveitar oportunidades. Esse trabalho pode variar dependendo das necessidades específicas de cada consultório e do escopo do trabalho. No entanto, geralmente, ele segue algumas etapas comuns, como descrevemos a seguir.

### *Registrar as atividades de tratamento*

O registro de uma operação de tratamento é similar à criação de um Procedimento Operacional Padrão (POP). O POP é um documento que descreve com detalhes todas as operações necessárias para a realização de uma tarefa no consultório médico, ou seja, um roteiro padronizado para realização dessas atividades, garantindo que qualquer pessoa consiga realizá-lo. Os POPs podem descrever diferentes procedimentos, como o atendimento ao paciente e a lavagem correta das mãos.

Ao longo do programa de governança, o encarregado irá registrar todos os processos que ocorrem em sua clínica, desde o atendimento ao cliente até as questões administrativas. Em cada um, indicará os dados tratados, os profissionais que possuem acesso a esses dados, onde são armazenados, as medidas de segurança, enfim, tudo o que for necessário para compreender a trajetória do dado pessoal.

### *Elaborar diagnóstico*

Após o mapeamento, que consiste em verdadeira "fotografia" do cenário de tratamento dos dados, deve ser conduzido um diagnóstico com base na LGPD. Uma das ações do diagnóstico é a eleição de bases legais para cada um dos fluxos. Essa atividade é especialmente importante, pois, como vimos, nenhuma atividade pode ocorrer sem que exista uma base legal correspondente, sob pena de se cometer uma infração à LGPD.

Nessa fase, também deve ser feita uma classificação de riscos. Processos que envolvam o tratamento de um grande volume de dados pessoais ou cujo tratamento possa (a) gerar risco de ofensa a direitos e garantias fundamentais, (b) envolvam o uso de tecnologias inovadoras, tecnologias de vigilância ou processos automatizados ou (c) envolvam dados de crianças ou idosos serão classificados como de alto risco, por critérios adotados pela ANPD, conforme a Resolução nº 02/2022.

Vale dizer que essa análise não é trivial, pois muitas incertezas ainda pairam sobre o assunto. Por exemplo, a definição do que é um grande volume de dados está em processo de definição pela ANPD (ou seja, ainda não há um parâmetro objetivo que permita uma compreensão sobre quantos pacientes ter para que se esteja diante de alto volume). Por isso, recomenda-se que o diagnóstico seja feito pelo encarregado/DPO.

### *Identificar lacunas e mitigar riscos*

O registro das atividades de tratamento e o diagnóstico dos processos, além de serem obrigatórios, têm um papel fundamental: auxiliar na identificação de lacunas dos processos e na mitigação de riscos. Por exemplo, ao mapear o processo de atendimento de cliente, é possível que se identifique que o prontuário do paciente esteja armazenado em uma gaveta sem chaves. Esse modo de armazenamento permite que terceiros mal-intencionados tenham acesso ao documento com facilidade. O encarregado sugerirá a aquisição de cadeados para que se crie uma camada física de segurança.

Outra lacuna recorrente no setor médico é o armazenamento de dados repetidos. Por exemplo, armazenar documentos do paciente no computador, e-mail ou *drive* e ainda os imprimir. Essa prática, apesar de aparentar maior segurança, pode gerar maior chance de ocorrência de um incidente de segurança, como um acesso indevido dos dados por terceiros, sem controle sobre todos os locais de armazenamento.

## Desafios e cuidados de um Programa de Governança em Proteção de Dados para médicos

Implementar um Programa de Governança em Proteção de Dados apresenta desafios para todos os setores. Mapear todos os processos, identificar os riscos e implementar as medidas corretivas são tarefas que merecem cuidado.

No setor médico, a implementação de um programa de governança possui alguns pontos de atenção especial. Para os fins deste artigo, dois pontos de atenção serão abordados: armazenamento de prontuários eletrônicos e registros de saúde e as relações entre o médico e as Operadoras de Saúde.

### *Prontuários Eletrônicos do Paciente (PEP) e Registros Eletrônicos de Saúde (RES)*

A digitalização das relações é uma tendência cada vez mais forte na medicina. Com o avanço das tecnologias digitais, os documentos tradicionais que antes estruturavam as informações do paciente, como o prontuário e os registros, passaram por processo de digitalização.

Por um lado, essa digitalização trouxe inúmeros benefícios aos médicos e pacientes pela facilidade de acesso aos dados. Por outro, gerou uma redundância de arquivos físicos e digitais, com alguns riscos de segurança[8]. Muitas vezes, a via física dos documentos digitalizados são mantidas em caixas ou arquivos sem grande controle, com risco de acesso indevido. Além disso, a lei prevê um prazo de guarda de documentos, após o qual devem ser eliminados. Sem um controle ativo, corre-se o risco de os documentos seguirem armazenados indefinida e indevidamente.

Se lhe causou uma surpresa saber que os dados pessoais possuem um tempo de guarda, vale saber que todo tratamento de dados está vinculado a uma finalidade. Os dados só podem ser usados enquanto

forem necessários para cumprir a finalidade informada. Uma vez cumprida a finalidade, devem ser eliminados, sob pena de violação à LGPD.

Por exemplo, imagine que você finalizou o atendimento de um paciente. Não há outras linhas de tratamento no caso e o prontuário não é movimentado há algum tempo. É possível dizer que a finalidade do tratamento dos dados se finalizou. A princípio, o término da finalidade justificaria a trituração do prontuário em papel. Entretanto, a Lei nº 13.787/18 determina que os prontuários em papel devam ser armazenados por um período mínimo de 20 anos, contados do último registro. Logo, o armazenamento agora tem a finalidade de atender à lei, mas, após o prazo legal, deverá ser cessado.

Assim como o prontuário, todos os documentos da clínica médica terão um prazo para ser descartados. A análise desses prazos e a criação de uma tabela de temporalidade, utilizada para gestão dos documentos, é uma das funções do Encarregado pelo Tratamento dos Dados.

Outra função relevante e relacionada aos prontuários eletrônicos é a análise dos fornecedores da clínica. É comum no meio médico a contratação de *softwares* que fazem a gestão dos prontuários médicos. A contratação de um *software* que não atenda aos requisitos da LGPD pode causar a responsabilização do médico, conforme visto anteriormente na seção "Responsabilidades do médico". Por isso, antes de contratar qualquer plataforma ou fornecedor, deve ser conduzida uma avaliação da empresa a ser contratada, com base em *checklist* de requisitos da LGPD – essa avaliação é chamada de "*due diligence* de fornecedores" e permite avaliar o grau de maturidade do parceiro no tema e os riscos daquela contratação.

### *Relação com operadoras de saúde*

Outro desafio para médicos diz respeito à interface com operadoras de saúde. Geralmente, o contrato de credenciamento assinado com as operadoras possui cláusulas específicas de proteção de dados que definem obrigações entre as partes. Assim, um médico que atende várias operadoras estará submetido a diversas regras contratuais sobre o tema.

Por exemplo, o contrato com a operadora "X" pode prever que, se ocorrer um incidente de segurança com os dados, o médico deve comunicar à operadora e tomar providências em prazo de até 72 horas. Já o contrato com a operadora "Z" estabelece prazo de 24 horas para as mesmas providências. É importante, portanto, que o médico possua um rígido controle acerca dessas obrigações para que não corra o risco de descumprir uma cláusula contratual.

É possível também que algumas operadoras de saúde exijam que todos os documentos de seus pacientes fiquem armazenados conforme regras específicas, em banco de dados segregados, por exemplo. Ao revisar o contrato, o encarregado identificará essas obrigações e, se necessário, fará uma análise de riscos das cláusulas contratuais.

Recomenda-se, portanto, que o médico esteja atento às cláusulas de proteção de dados no momento do credenciamento.

## Seguros de responsabilidade civil

O seguro de responsabilidade civil é uma forma de proteção financeira que os profissionais, incluindo médicos, podem adquirir para se proteger contra reclamações de responsabilidade civil e os custos associados a processos judiciais. O seguro cobre os custos de defesa legal, indenizações e acordos judiciais em caso de reclamações de negligência médica.

### *Possíveis seguros para médicos*

Como se sabe, médicos enfrentam diversos riscos em sua prática diária que podem afetar tanto a sua carreira quanto o bem-estar dos seus pacientes. Esses riscos variam desde a ocorrência de erro médico (que pode levar a processos judiciais), até problemas na infraestrutura de segurança de TI das clínicas e consultórios. Nesse contexto, os seguros para médicos surgem como uma ferramenta recomendável para a proteção financeira e profissional, trazendo maior tranquilidade e segurança no exercício da profissão.

Existem diversos tipos de seguros que podem contribuir para trazer conforto aos profissionais de saúde. Dentre eles, destacam-se os relacionados abaixo.

– *Seguro de responsabilidade civil profissional:* seguro com o propósito de proteger os médicos contra reivindicações de danos causados por erros, omissões ou negligência no exercício da medicina. Podem cobrir custos legais, indenizações e outros gastos relacionados a processos judiciais.
– *Seguro de equipamentos e infraestrutura:* cobre danos ou perdas de equipamentos médicos devido

a roubo, incêndio, ou outros eventos imprevistos.

– *Seguro de saúde e vida:* oferecem proteção financeira para os médicos e suas famílias em caso de doenças graves, acidentes ou morte.
– *Seguros cibernéticos:* oferecem cobertura contra riscos associados à tecnologia da informação e à privacidade de dados. Ele é projetado para ajudar os médicos a mitigar as consequências de incidentes cibernéticos, como vazamentos de dados, ataques de *ransomware*, ou violações de segurança.

Sobre essa última modalidade, valem algumas considerações.

### *Seguros cibernéticos*

Com a crescente digitalização na área da saúde, a segurança cibernética tornou-se uma preocupação central. Como visto, os dados dos pacientes podem ser sensíveis e valiosos, tornando-se alvos frequentes de ataques cibernéticos. Além disso, vazamentos podem resultar em graves consequências legais, financeiras e de reputação para os médicos e suas clínicas.

Para prevenir esses riscos, pode fazer sentido contratar um bom seguro cibernético, que geralmente inclui as ocorrências descritas a seguir.

– Custos de resposta a incidentes: cobre os gastos necessários para responder a um ataque cibernético, incluindo a contratação de especialistas em TI para conter e resolver o problema.
– Notificação e monitoramento de crédito: custos associados à notificação de pacientes sobre o vazamento de dados e serviços de monitoramento de crédito para evitar fraudes.
– Responsabilidade por privacidade e segurança de dados: protege contra ações legais e multas decorrentes de falhas na proteção de dados pessoais.
– Perdas de receita e recuperação de dados: compensa pela perda de receitas devido a interrupções operacionais e cobre os custos de restauração de dados perdidos.

Os médicos devem considerar o seguro cibernético como uma parte importante de sua estratégia de gerenciamento de riscos. Com a adoção crescente dos documentos e prontuários eletrônicos e dos sistemas digitais de gestão de pacientes, a probabilidade de sofrer um ataque cibernético aumenta significativamente.

Ao investir em uma cobertura abrangente, os médicos podem focar no que fazem de melhor – cuidar da saúde de seus pacientes – enquanto permanecem protegidos contra os diversos riscos que a profissão apresenta.

## Conclusão

A LGPD trouxe um novo paradigma para o tratamento de dados pessoais no Brasil, afetando significativamente diversos setores, incluindo a área da saúde. As clínicas médicas, que lidam diariamente com diferentes informações de pacientes, precisam adaptar-se a essa legislação para garantir a proteção adequada dos dados e evitar consequências severas.

Como visto, dados pessoais são todas as informações relacionadas a uma pessoa física identificada ou identificável, enquanto dados sensíveis incluem informações que podem causar discriminação, como origem racial, convicção religiosa, opinião política e dados de saúde. A LGPD impõe uma camada adicional de proteção para os dados sensíveis, restringindo suas hipóteses de uso.

O tratamento de dados pessoais, por sua vez, é conceito relevante que abrange uma série de ações, desde a coleta e armazenamento até o processamento e compartilhamento dos dados. Cada uma dessas atividades deve ser realizada com base em uma justificativa legal adequada. Entre as bases legais mais relevantes para o setor médico, estão o consentimento do paciente, o cumprimento de obrigações legais e regulatórias, a execução de contratos e a tutela da saúde. A escolha da base legal correta é crucial, pois uma escolha inadequada pode resultar em infrações à LGPD.

Os médicos e clínicas precisam estar cientes das responsabilidades administrativas, judiciais e contratuais que o não cumprimento da LGPD pode acarretar. Administrativamente, a ANPD pode aplicar sanções que variam de advertências a multas significativas, além da possível suspensão das atividades de tratamento de dados. Judicialmente, a responsabilidade civil pode resultar em condenações por danos morais e materiais, dependendo das consequências do vazamento ou uso indevido dos dados. Contratualmente, podem estar previstas penalidades em caso de descumprimento das cláusulas de proteção de dados.

Para mitigar esses riscos e assegurar a conformidade com a LGPD, a implementação de um Programa de Governança em Proteção de Dados é essencial. Um programa de governança deve ser contínuo e

incluir o monitoramento constante das atividades de tratamento de dados, a definição de medidas de segurança apropriadas, e o registro detalhado das operações de tratamento. O encarregado pelo tratamento dos dados pessoais desempenha um papel central nesse processo, sendo responsável por garantir que todas as atividades estejam em conformidade com a legislação vigente.

Além disso, a digitalização das informações médicas, como os Prontuários Eletrônicos do Paciente (PEP) e os Registros Eletrônicos de Saúde (RES), exige uma atenção especial. A escolha de fornecedores que atendam aos requisitos da LGPD e a gestão adequada do ciclo de vida dos dados são medidas importantes para evitar infrações e proteger a privacidade dos pacientes.

Em conclusão, a conformidade com a LGPD é um desafio complexo e contínuo para as clínicas médicas. No entanto, com a implementação de um robusto Programa de Governança em Proteção de Dados e a adoção de medidas de segurança apropriadas, é possível garantir a proteção dos dados dos pacientes, evitando penalidades e fortalecendo a confiança no serviço prestado. Investir em conformidade não só evita sanções legais, mas também promove uma prática médica ética e responsável, beneficiando tanto os profissionais de saúde quanto seus pacientes.

## Referências

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]. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon4CDANPD24.02.2023.pdf. Acessado em: 27/05/2024.
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]. Disponível em: https://portal.cfm.org.br/noticias/publicidade-medica-justica-mantem-decisao-do-cfm-e-do-cremec-contra-medico-que-violava-preceitos-eticos/. Acessado em 24/05/2024.
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.

Não foram declarados conflitos de interesse associados à publicação deste artigo.

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