



**Universidade Federal de Minas Gerais
Faculdade de Ciências Econômicas
Departamento de Ciências Administrativas
Curso de Especialização em Gestão Estratégica em Saúde**

FÁBIO CÂMARA DO AMARAL

**LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: PROTEÇÃO E
COMPARTILHAMENTO DE DADOS NA ÁREA DA SAÚDE.**

BELO HORIZONTE

2021

FÁBIO CÂMARA DO AMARAL

**LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: PROTEÇÃO E
COMPARTILHAMENTO DE DADOS NA ÁREA DA SAÚDE**

Trabalho de Conclusão do Curso de Especialização em
Gestão Estratégica de Saúde, do Departamento de Ciências
Administrativas da Faculdade de Ciências Econômicas-
UFMG

Orientadora: Prof.^a Dra. Márcia Mascarenhas Alemão

BELO HORIZONTE

2021

Ficha catalográfica

A4851
2021 Amaral, Fábio Câmara do.
 Lei geral de proteção de dados pessoais [manuscrito] : proteção e
 compartilhamento de dados na área da saúde / Fábio Câmara do
 Amaral. – 2021.
 17 f.: il.

 Orientadora: Márcia Mascarenhas Alemão.
 Monografia (especialização) – Universidade Federal de Minas
 Gerais, Centro de Pós-Graduação e Pesquisas em Administração.
 Inclui bibliografia (f. 16-17).

 1. Saúde – Administração. I. Alemão, Márcia Mascarenhas. II.
 Universidade Federal de Minas Gerais. Centro de Pós-Graduação e
 Pesquisas em Administração. III. Título.

CDD: 658



Universidade Federal de Minas Gerais
Faculdade de Ciências Econômicas
Departamento de Ciências Administrativas
Curso de Especialização em Gestão Estratégica em Saúde

ATA DA DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO do Senhor **FÁBIO CÂMARA DO AMARAL**, matrícula nº 2019665004. No dia 26/08/2021 às 17:00 horas, reuniu-se em sala virtual, a Comissão Examinadora de Trabalho de Conclusão de Curso, indicada pela Comissão de Coordenação Didática do Curso de Especialização em Gestão Estratégica em Saúde, para julgar o Trabalho de Conclusão de Curso intitulado "**LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: PROTEÇÃO E COMPARTILHAMENTO DE DADOS NA ÁREA DA SAÚDE.**", requisito para a obtenção do Título de Especialista. Abrindo a sessão, a Orientadora e Presidente da Comissão, Prof^a Márcia Mascarenhas Alemão, após dar conhecimento aos presentes do teor das Normas Regulamentares de apresentação do TCC, passou a palavra ao aluno para apresentação de seu trabalho. Seguiu-se a arguição pelos examinadores, seguido das respostas do aluno. Logo após, a Comissão se reuniu sem a presença do aluno e do público, para avaliação do TCC, que foi considerado:

(x) APROVADO

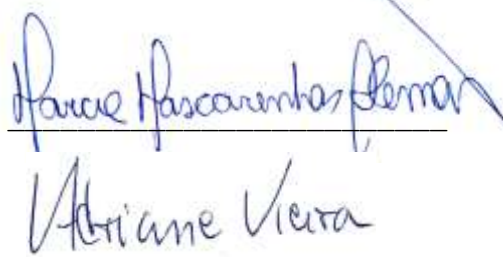
() NÃO APROVADO

90 pontos (noventa pontos). Trabalhos com nota maior ou igual a **60** serão considerados aprovados.

O resultado final foi comunicado publicamente ao aluno pela orientadora e Presidente da Comissão. Nada mais havendo a tratar, a Senhora Presidente encerrou a reunião e lavrou a presente ATA, que será assinada por todos os membros participantes da Comissão Examinadora. Belo Horizonte, 26/08/2021.

Prof^a Márcia Mascarenhas Alemão
(FHEMIG - Orientadora)

Prof^a Dra. Adriane Vieira
(DGSS/ ENF/UFMG)



Márcia Mascarenhas Alemão
Adriane Vieira

RESUMO

A Lei nº 13.719/2018 é um novo marco para a proteção de dados pessoais, e se aplica a todas as empresas públicas e privadas, independente do ramo em que elas atuam. A Lei Geral de Proteção de Dados Pessoais (LGPD) dispõe sobre o tratamento de dados pessoais por pessoal natural ou jurídica de direito público ou privado, protegendo dados físicos quando os obtidos por meio digital e foi promulgada em 14 de agosto de 2018 e entrou em vigor em 18 de setembro de 2020, porém as sanções administrativas só passaram a vigorar em agosto de 2021. A LGPD busca o equilíbrio entre o uso de dados pessoais e a proteção à privacidade. E confere obrigações diferenciadas para esses dados e consequentemente um padrão de proteção maior. O impacto da nova legislação na área da saúde é grande, os dados de saúde são considerados sensíveis, pois, podem gerar riscos aos direitos e liberdades fundamentais e por este motivo a lei os trata com mais rigor. Este trabalho apresenta alguns conceitos sobre a proteção de dados na área da saúde, e tem como principal objetivo discutir a necessidade de se proteger os dados pessoais no ambiente hospitalar, apontando as dificuldades de adequação à nova legislação. É estruturado com base na seguinte pergunta de pesquisa: O setor da saúde pode compartilhar os dados do paciente? O desenvolvimento do artigo está pautado na revisão narrativa de literatura.

Palavras-chave: Lei. Dados Pessoais. Proteção. Compartilhamento.

ABSTRACT

Law No. 13,719 / 2018 is a new milestone for the protection of personal data, the law applies to all companies regardless of the industry in which they operate, both for private and public companies. The law provides for the protection of personal data and was known by the acronym LGPD, that is, the General Law for the Protection of Personal Data, was enacted by the then President of the Republic Michel Temer on August 14, 2018, however, it only came into force on September 18, 2020, but administrative sanctions will only take effect August 2021. The law seeks a balance between the use of personal data and the protection of privacy. The LGPD provides for the processing of personal data by a natural person or a legal person under public or private law, protecting both physical and digital data. The impact of the new legislation in the area of health is great, health data are considered by the law as sensitive data, the law confers different obligations on these data and, consequently, greater protection of these data. Sensitive data can generate risks to fundamental rights and freedoms and for this reason the law treats them more rigorously. Thus, this paper presents a debate on data protection in the health area, and its main objective is to debate the need for protect personal data in the hospital environment, pointing out the difficulties in adapting to the new legislation. Thus, the work is structured based on the following question as a problem: Can the health sector share patient data? The development of the article is based on the qualitative research technique of exploratory character and bibliographic survey.

Keywords: Law. Personal Data. Protection. Sharing.

SUMÁRIO

1. INTRODUÇÃO.....	5
2. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS LGPD	6
2.1. Definição	6
2.2. A quem se aplica.....	6
2.3. Conceitos essenciais da LGPD – Tratamento de dados, dados pessoais, dados pessoais sensíveis, consentimento e eliminação	7
2.4. Quem é quem na LGPD	8
2.5. Direitos trazidos pela nova legislação	9
3. PROTEÇÃO E COMPARTILHAMENTO DE DADOS NA ÁREA DA SAÚDE.....	11
3.1. Compartilhamento de dados de saúde	11
3.2. Compartilhamento com outros profissionais da saúde	12
4. CONSIDERAÇÕES FINAIS	15
REFÊNCIAS	16

1 INTRODUÇÃO

Com a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) o Brasil passou a fazer parte do rol de países que possuem uma legislação voltada à proteção de dados pessoais. A LGPD foi inspirada no Regulamento Geral sobre Proteção de Dados – RGPD, legislação europeia que protege a privacidade dos cidadãos diante das empresas, oferecendo aos proprietários dos dados pessoais maior controle e transparência sobre os dados tratados pelas empresas.

A Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD (BRASIL, 2018), regulamenta todo os aspectos relacionados ao uso de dados pessoais, por pessoas físicas e jurídicas. A legislação traz mudanças expressivas no contexto do tratamento de dados pessoais, determinando como as empresas, hospitais, clínicas médicas, laboratórios, instituições de ensino, associações e o poder público deverão coletar, armazenar, utilizar, compartilhar e eliminar os dados pessoais no desempenho de suas atividades.

A lei aplica-se independentemente do meio e/ou forma de tratamento dos dados, seja físico ou digital. A LGPD regula todas as operações de tratamento de dados realizadas no Brasil com objetivos econômicos.

O objetivo da lei é proteger os direitos fundamentais de liberdade e privacidade, trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais, incluindo a categoria de dados sensíveis.

Qualquer estabelecimento hospitalar possui informações confidenciais, tanto de pacientes quanto de seus colaboradores, médicos e prestadores de serviço. Os hospitais, devido à complexidade dos processos tem um longo caminho a percorrer e precisarão tomar muitas providências com o objetivo de garantir a segurança e privacidade de dados de seus pacientes, colaboradores, médicos e também de seus prestadores de serviços, sem que isso interfira na assistência aos pacientes.

Assim, o presente artigo visa responder à seguinte pergunta de pesquisa: quais os impactos da Lei Geral de Proteção de Dados Pessoais na área hospitalar especialmente em relação ao compartilhamento de dados de saúde. Buscando responder a esta questão, o objetivo deste artigo é descrever os impactos da Lei Geral de Proteção de Dados Pessoais – LGPD na área hospitalar, especialmente em relação ao compartilhamento de dados de saúde. Trata-se de uma revisão narrativa de literatura.

2. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

2.1 DEFINIÇÃO DA LEI

A Lei Geral de Proteção de Dados Pessoais (LGPD) regulamenta todos os aspectos relativos ao uso de dados pessoais e foi promulgada em 14 de agosto de 2018 (BRASIL, 2018) e tem como objetivo garantir ao cidadão a proteção de seus dados confiados às empresas, alterando o Marco Civil da Internet Lei nº 12.965/14. O propósito da nova legislação é definir de forma clara a responsabilidade de quem coleta, armazena e trata dados de pessoas físicas, impondo limites e punições, inclusive pecuniárias para casos de vazamentos ou violações de dados pessoais.

A LGPD traz mudanças profundas e significativas no contexto do tratamento de dados pessoais, determinando como as empresas deverão se comportar em relação aos dados pessoais.

A lei brasileira tem como fonte a GDPR – Regulamento Geral de Proteção de Dados da União Europeia (EU, 2016). A legislação europeia foi publicada em 2016, com vigência em maio de 2018 e afetou diversas nações, inclusive o Brasil que no mesmo ano criou LGPD.

A proteção de dados no Brasil não é algo novo, podemos citar vários dispositivos, como por exemplo: a Constituição Federal de 1988 (BRASIL, 1988), o Código de Defesa do Consumidor (BRASIL, 1990), a resolução 1.821/07 do CFM, o Decreto 6.135/07 – Cadastro Único de Programa Sociais, o Decreto 6.523/07 – Serviço de SAC, o Decreto 6.425/08 – Censo Anual da Educação, Lei 12.414/11 (BRASIL, 2011) – Cadastro Positivo, a Lei 12.527/11 (BRASIL, 2011) – Lei de Acesso à Informação, a Lei 12.737/12 (BRASIL, 2012) – Lei de Invasão de Dispositivos, Decreto 7.962/13 – Comércio Eletrônico, Lei 12.965/14 – Marco Civil da Internet, Decreto 8.777/16 – Política de Dados Abertos do Governo Federal e em 2018 a Lei 13.709 – Lei Geral de Proteção de Dados Pessoais - LGPD, tema deste trabalho.

Por mais que vivenciamos a era digital, onde muitas vezes os dados já nascem de forma digital, são utilizados e descartados diretamente por meios digitais a LGPD também se aplica ao tratamento de dados em estado físico, ou seja, dados que estejam em papel.

2.2 A QUEM SE APLICA A LGPD?

A LGPD se aplica a qualquer pessoa – natural ou jurídica de direito público ou privado, que realize tratamento de dados pessoais, ou seja, exerça atividades econômicas que utilizem dados pessoais, por meio digital ou físico. Dessa forma, a lei se aplica a todas as empresas e afeta todos os cidadãos (MACIEL, 2019).

A legislação brasileira orienta e coordena as ações das empresas quanto ao processamento justo e adequado de dados pessoais e as responsabiliza pela guarda e uso seguro dos dados de seus clientes, funcionários e prestadores de serviço, entre outros (MACIEL, 2019). Para o melhor entendimento da LGPD, veremos a seguir alguns conceitos trazidos pela lei.

2.3 CONCEITOS ESSENCIAIS DA LGPD – TRATAMENTO DE DADOS, DADOS PESSOAIS, DADOS PESSOAIS SENSÍVEIS, CONSENTIMENTO E ELIMINAÇÃO.

A LGPD alcança o tratamento de dados pessoais independente de quem os realize. O artigo 5º, X da lei conceitua tratamento de dados nos seguintes termos:

“Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” (BRASIL, 2018).

Nos termos da Lei, tratamento de dados tem um sentido muito amplo, o artigo 5º, X, traz uma lista exemplificativa e não taxativa. Qualquer ação digital ou física que tenha como objeto qualquer dado pessoal pode ser caracterizado como tratamento.

Por seu turno, dado pessoal é qualquer informação relacionada a uma pessoa natural, que permite ou contribua para a sua identificação, como por exemplo: nome, CPF, endereço, dados biométricos, entre outros. Informações abstratas e relativas as pessoas jurídicas estão fora do conceito de dado pessoal e do escopo da LGPD. O dado pessoal se caracteriza com o vínculo de uma informação a um indivíduo. O vínculo deriva de uma identificação entre o dado e o indivíduo. Por exemplo, o número de um determinado CPF indica uma determinada pessoal, assim como os dados biométricos.

Superado o conceito de dado pessoal, passamos agora a compreensão do conceito de dado pessoal sensível, nos termos da LGPD. O Artigo 5, II define dado pessoal sensível da seguinte forma:

“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” (BRASIL, 2018);

A lista é taxativa e não admite outras definições. Destaca-se a inclusão de dado referente à saúde como sensíveis. O Artigo 5, II dá o embasamento suficiente para compreendermos que todos os dados presentes em prontuários médicos e outros documentos de uso hospitalar, como,

receitas, ficha de atendimento, anamneses, resultados de exames, fazem parte do conjunto de dados sensíveis, entabulado no respectivo artigo e merecem tratamento diferenciado pela lei.

O consentimento é uma das dez bases legais previstas na lei, e devido a sua transparência ante ao titular é a situação que traz maior segurança jurídica para o controlador, assim como para o operador, uma vez que o titular do dado autoriza o tratamento. O consentimento está definido no Artigo 5º, XII, nos seguintes termos: “Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (BRASIL, 2018); São elementos do consentimento: a liberdade da manifestação; consciência bem informada do titular do dado; e caráter inequívoco da manifestação. De forma simples, o consentimento é a manifestação livre, informada e consciente pela qual o titular do dado concorda com o tratamento de seus dados para uma finalidade determinada, ou seja, específica.

A exclusão de dados ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado é conceituado pela lei como eliminação ou exclusão. A LGPD orienta que ao final do tratamento, os dados deverão ser eliminados, porém a própria lei define situações em que a conservação é admitida, e muitas vezes obrigatórios por força de lei. Vejamos: (I) cumprimento de obrigação legal, (II) estudos por órgãos de pesquisa, (III) transferência a terceiro, desde que respeitado os requisitos da lei e (IV) uso exclusivo do controlador, desde que os dados sejam anonimizados. Assim, mesmo que o titular do dado deseje a eliminação, poderá haver a manutenção dos dados para as finalidades descritas acima.

A lei segrega o conceito de dado pessoal, o qual se entende como toda informação relacionada a pessoa natural (física) identificada ou identificável do conceito de dado pessoal sensível caracterizados como aqueles que geram maior discriminação ao titular dos dados, ou seja, podem causar maior dano.

2.4 QUEM É QUEM NA LGPD?

O titular dos dados pessoais é o núcleo de toda existência da LGPD. O titular dos dados pessoais é a pessoa física proprietária dos dados pessoais protegidos pela lei.

Controlador é a pessoa jurídica ou natural, de direito público ou privado, a quem compete as decisões referentes ao tratamento dos dados pessoais. A LGPD impõe o seu maior peso jurídico sobre o controlador, pois ele é o responsável pela tomada de decisões e, operador é a pessoa jurídica ou natural, de direito público ou privado que realiza o tratamento de dados pessoais em nome do controlador.

O operador age conforme diretrizes traçadas pelo controlador, não tendo qualquer interferência sobre o tratamento dos dados do titular, é o controlador quem define as finalidades do tratamento dos dados pessoais, por este motivo a lei impõe maior peso a ele.

Grande parte das obrigações recai, sobre o controlador, uma vez que é ele quem possui relação direta com o titular dos dados. Ao operador recai obrigações acessórias, definidas em contrato firmado com o controlador.

Encarregado de Dados Pessoais corresponde a pessoa física ou jurídica contratada ou nomeada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados– ANPD (BRASIL, 2018). Outra função do encarregado é orientar o controlador no processo de tratamento de dados, este profissional tem caráter consultivo dentro da organização.

ANPD é o órgão responsável pelo zelo, implemento e fiscalização do cumprimento da Lei Geral de Proteção de Dados Pessoais.

2.5 DIREITOS TRAZIDOS PELA NOVA LEGISLAÇÃO

O legislador cuidou de definir as responsabilidades daqueles que realizam o tratamento dos dados, mas também listou diversos direitos dos titulares. O artigo 17 da Lei Geral de Proteção de Dados Pessoais assegura a todas as pessoas naturais a titularidade de seus dados e garante a eles os direitos fundamentais de liberdade e privacidade.

O Artigo 18, estabelece os direitos do titular, vejamos:

“Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

- I - confirmação da existência de tratamento;
- II - acesso aos dados;
- III - correção de dados incompletos, inexatos ou desatualizados;
- IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
- V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
- VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei” (BRASIL, 2018):

A legislação brasileira estipula uma série de condutas a serem seguidas em relação aos titulares dos dados pessoais.

O Artigo 42 da Lei estabelece responsabilidades ao controlador e operador, vejamos:

“O controlador ou o operador que, em razão do exercício da atividade de tratamento de dados causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação é obrigado a repará-lo”.

Na área da saúde os dados pessoais sensíveis circulam e precisam circular para garantir a melhor assistência, com o objetivo maior de reestabelecer a saúde do paciente.

Realizado o estudo dos conceitos essenciais da Lei Geral de Proteção de Dados, veremos a seguir pontos específicos que dizem respeito ao compartilhamento de dados na área da saúde.

3. PROTEÇÃO E COMPARTILHAMENTO DE DADOS NA ÁREA DA SAÚDE

3.1 COMPARTILHAMENTO DE DADOS DE SAÚDE

Os dados de saúde são considerados pela LGPD dados sensíveis, recebendo tratamento especial da lei conforme Artigo 5º que apresenta que:

“II - 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” (BRASIL, 2018)

Tais dados representam a extensão da personalidade do indivíduo e quando utilizados de forma irregular podem acarretar danos incalculáveis ao titular dos dados, pois são dados que geram maior discriminação/danos (MACIEL 2019).

Na área da saúde os dados precisam ser compartilhados com todos os indivíduos dentro da cadeia de cuidado, melhor dizendo, é preciso que todas as pessoas envolvidas no reestabelecimento da saúde do paciente tenham o amplo acesso aos dados, como por exemplo: exames laboratoriais, exames de imagem, histórico de doenças, entre outros, tudo para a adequada tutela da saúde do paciente (DALLARI e MONACO, 2021).

A LGPD evidência a exceção da obrigatoriedade do consentimento para situações exclusiva da tutela da saúde e para a proteção da vida ou incolumidade física do titular ou de terceiros. Isto quer dizer que, a dispensa do consentimento do paciente justifica-se em caso de tratamento de saúde, desde que seja em situações de urgência e/ou emergência, situações em que a vida do paciente esteja em risco. O tratamento e o compartilhamento de dados de saúde sem o consentimento do titular é exceção, e não regra (DALLARI e MONACO, 2021).

Assim, é vedado o compartilhamento de dados de saúde para pessoas jurídica que não estejam envolvidas no dever de cuidado do paciente. Da mesma forma, é expressamente proibido o compartilhamento de dados sensíveis referentes à saúde com o objetivo de obter vantagem econômica (DALLARI e MONACO, 2021).

Daí a importância de que todas as atividades de tratamento de dados pessoais sensíveis referentes à saúde observem os princípios estampados no artigo 6º da lei – boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção e não discriminação (DALLARI e MONACO, 2021).

Assim, o esforço passa a ser o de tratar os dados pessoais dos pacientes de forma a atender todos os princípios entabulados no Artigo 6º da lei. O princípio da finalidade tem grande

relevância prática, ele garante ao titular as fronteiras de legalidade do tratamento de seus dados, em outras palavras garante que os dados sejam utilizados conforme foi autorizado. O princípio da adequação está estritamente ligado ao da finalidade, uma vez que, prevê que o tratamento de dados somente pode ocorrer quando houver compatibilidade com as finalidades (DALLARI e MONACO, 2021).

A necessidade do tratamento também está relacionada de forma direta aos dois princípios anteriores, visto que ressalta a licitude do tratamento de dados pessoais de acordo com a finalidade. O controlador, além de informar o titular acerca do tratamento precisa garantir o livre acesso aos seus próprios dados, assim como a integridade e a qualidade dos dados, principalmente os dados de saúde (DALLARI e MONACO, 2021).

O dever de transparência obriga o controlador a prestar informações claras, precisas e facilmente acessíveis sobre a realização do tratamento dos dados do titular. Somente o titular ou pessoa autorizada podem ter acesso aos seus dados.

A segurança e prevenção não estão limitadas às medidas tecnológicas, mas também a medidas administrativas aptas a evitar incidentes, é preciso que o estabelecimento de saúde crie normas e políticas que garantam a proteção dos dados. Nenhum dado coletado poderá ser tratado para fins discriminatórios ilícitos ou abusivos.

Dessa forma, o compartilhamento de dados com outros estabelecimentos de saúde é lícito, desde que observados os dispositivos, princípios e fundamentos da legislação.

3.2 COMPARTILHAMENTO COM OUTROS PROFISSIONAIS DA SAÚDE

O compartilhamento de dados pessoais sensíveis referentes à saúde, não é possível sem o consentimento do paciente titular do dado, mesmo que entre médicos, a não ser que os outros profissionais da saúde estejam diretamente ligados à assistência do paciente, devendo observar as hipóteses legais previstas na LGPD.

Assim, o acesso ilimitado aos dados do paciente, por médicos, enfermeiros e outros profissionais da área da saúde, sem o envolvimento direto com a assistência do paciente titular dos dados, representa tratamento irregular ao teor da lei, sendo o controlador responsável pela violação.

Sigilo, privacidade e segurança não são conceitos novos na área da saúde, mas não é por isso que os serviços de saúde não devam investir em ferramentas administrativas e técnicas para proteger os dados pessoais, pois a partir da LGPD tais conceitos ganham ainda mais importância no setor da saúde.

Para garantir os padrões de boas práticas é recomendável que as empresas de todos os segmentos adotem programas boas práticas e de governança, nos termos do Artigo 50 da LGPD, vejamos:

“Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

- a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
- b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
- c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
- d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
- f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
- g) conte com planos de resposta a incidentes e remediação; e
- h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta,

os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.” (BRASIL, 2018)

O programa de boas práticas e de governança deve demonstrar o comprometimento do controlador e/ou operador em adotar processos e normas internas que assegurem o cumprimento de boas práticas relativas à proteção de dados pessoais. O programa de boas práticas e governança deverão ser publicados e atualizados periodicamente.

4. CONSIDERAÇÕES FINAIS

A LGPD responsabiliza pessoas físicas e jurídicas pela guarda e uso dos dados pessoais de seus clientes, colaboradores e prestadores de serviço, entre outros. Médicos em seus consultórios, hospitais, clínicas, laboratórios e centros de diagnósticos, todos estão submetidos às definições de proteção de dados tratada pela lei, assim como estão sujeitos às punições previstas para casos de infração.

Mesmo que a confidencialidade já faça parte do dia a dia dos profissionais da saúde, é preciso que o setor crie normas e diretrizes que garantam a aplicação de todos os conceitos trazidos pela Lei. Os dados dos pacientes é um bem essencial para as atividades dos estabelecimentos de saúde e até mesmo para a uma adequada prestação de serviço.

A LGPD trouxe novas responsabilidades, direitos e deveres e é fundamental que os estabelecimentos criem políticas e normas alinhadas às boas práticas de uso de dados, com o objetivo de garantir níveis adequados de proteção aos dados dos pacientes, bem como o envolvimento de todos os profissionais da saúde que participam do processo de cuidado. Além da criação de políticas e normas o desenvolvimento de um bom programa de governança é de suma importância para mitigação dos riscos e de potenciais danos.

A Lei prevê as bases legais para tratamento de dados pessoais. As bases legais são os meios pelos quais o tratamento do dado é justificado. Dessa forma, para que haja o legítimo tratamento do dado, há necessariamente, que se definir uma base legal para o tratamento.

O termo de consentimento permanece como uma das bases legais para o tratamento dos dados de saúde. Entretanto, a LGPD evidencia algumas exceções da obrigatoriedade do consentimento, como por exemplo, situações exclusiva da tutela da saúde e para a proteção da vida ou incolumidade física do titular ou de terceiros, desde que seja em situações classificadas como urgentes e/ou emergentes, onde a espera pelo consentimento certamente colocaria em risco a vida do titular, da mesma maneira o compartilhamento de dados com os profissionais envolvidos no cuidado sem o devido consentimento também é uma exceção, não sendo viável o compartilhamento dos dados com profissionais que não estejam envolvidos diretamente na assistência do paciente titular do dado.

O compartilhamento de dados de saúde com outros estabelecimentos e profissionais de saúde é lícito, entretanto, há de se considerar os princípios e fundamentos entabulados na LGPD demais dispositivos legais pertinentes.

REFERÊNCIAS

Brasil, Presidência da República. *Decreto n. 6.135, de 26 de junho de 2007. Dispõe sobre o Cadastro Único para Programas Sociais do Governo Federal e dá outras providências.*

Brasília, DF: Diário Oficial da União.

Brasil, Presidência da República. *Decreto n. 6.523, de 31 de julho de 2008. Regulamenta a Lei no 8.078, de 11 de setembro de 1990, para fixar normas gerais sobre o Serviço de Atendimento ao Consumidor - SAC.* Brasília, DF: Diário Oficial da União.

Brasil, Presidência da República. *Decreto n. 6.425, de 4 de abril de 2008. Dispõe sobre o censo anual da educação.* Brasília, DF: Diário Oficial da União.

Brasil, Presidência da República. *Decreto n. 7.962, de 15 de março de 2013. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico.* Brasília, DF: Diário Oficial da União.

Brasil, Presidência da República. *Decreto n. 8.777, de 11 de maio de 2016. Institui a Política de Dados Abertos do Poder Executivo federal.* Brasília, DF: Diário Oficial da União.

Brasil. Conselho Federal de Medicina. *Resolução n. 1.821, de 23 de novembro de 2007. Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação Identificada em saúde.* Brasília, DF: Diário Oficial da União.

Brasil, Presidência da República. *Lei n. 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor.* Brasília, DF: Diário Oficial da União.

Brasil, Presidência da República. *Lei n. 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.* Brasília, DF: Diário Oficial da União.

Brasil, Presidência da República. *Lei n. 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.* Brasília, DF: Diário Oficial da União.

Brasil, Presidência da República. *Lei n. 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.* Brasília, DF: Diário Oficial da União.

Brasil, Presidência da República. *Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.* Brasília, DF: Diário Oficial da União.

Brasil, Presidência da República. *Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).* Brasília, DF: Diário Oficial da União.

Brasil, Presidência da República. *Constituição da República Federativa do Brasil de 1988.* Brasília, DF: Diário Oficial da União.

Ferreira, F. N. F., & Araújo, M. T. *Política de segurança da informação.* 2. ed. Rio de Janeiro: Ciência Moderna, 2008.

DALLARI, Analluza Bolivar. MONACO, Gustavo Ferraz de Campos. *LGPD na Saúde.* Thomson Reuters Brasil, São Paulo, 2021.

MACIEL, Rafael Fernandes. *Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18)* 1.ed. Goiânia – GO: RM Digital Education, 2019.

MALDONADO, Viviane Nóbrega. BLUM, Renato Opice. *LGPD: Lei Geral de Proteção de Dados comentada.* Thomson Reuters Brasil, São Paulo, 2019.

PECK Pinheiro, P. *Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD).* São Paulo: Saraiva, 2018.