CRM DF

LGPD

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Manual sobre a Lei Geral de Proteção de Dados Pessoais: LGPD

Conselho Federal de Medicina do Distrito Federal - CRMDF
Setor de Indústrias Gráficas (SIG), Quadra 01 Lote 985
Centro Empresarial Parque Brasília, Sala 202
Brasília-DF - CEP: 70.610-410
Tel: (61) 3322-0001 / email: crmdf@crmdf.org.br

Versão digital disponível em: www.crmdf.org.br

Coordenação geral: Farid Buitrago Sánchez e Carlos Guilherme Figueiredo
Autores: Farid Buitrago Sánchez, Carlos Guilherme Figueiredo e Lia Tolentino Corker Freire

Jornalista editora: Ludmila Mendonça Vaz
Revisora: Ludmila Mendonça Vaz
Imagens e ilustrações: Freepik
Projeto gráfico e diagramação: Diagraf Comunicação
Tiragem: 1.000 exemplares

Catalogação na fonte: Biblioteca do CFM

Conselho Regional de Medicina do Distrito Federal

Manual sobre a Lei Geral de Proteção de Dados Pessoais: LGPD / Farid Buitrago Sánchez, Carlos Guilherme Figueiredo e Lia Freire, coordenadores. Brasília: CRM-DF, 2022.

24 p. ; 15X21cm

ISBN 978-65-991837-2-0

1- LGPD. 2 - Direito à privacidade. 3 – Dados pessoais. 4 - Proteção de dados. 5 - Leis e legislação. I. Título.

CDD 342.721

Conselho Regional de Medicina do Distrito Federal

GESTÃO 2018/2023
DIRETORIA

GESTÃO 2018/2022

Presidente:
FARID BUITRAGO SÁNCHEZ
Vice-Presidente:
SÉRGIO TAMURA
1ª Secretária:
MARCELA A. MONTANDON GONÇALVES
2º Secretário:
PROCÓPIO MIGUEL DOS SANTOS
Tesoureiro:
CARLOS GUILHERME DA SILVA FIGUEIREDO

GESTÃO 2022/2023

Presidente:
MARCELA A. MONTANDON GONÇALVES
Vice-Presidente:
LEONARDO PITTA
1º Secretário:
FARID BUITRAGO SÁNCHEZ
2ª Secretária:
EDNA MÁRCIA XAVIER
Tesoureiro:
CARLOS GUILHERME DA SILVA FIGUEIREDO

Conselheiros:

ALÉCIO DE OLIVEIRA E SILVA
ALEXANDRE CHERMAN
ALÍPIO DE SOUSA NETO
CARLOS GUILHERME DA SILVA FIGUEIREDO
CAROLINE DA CUNHA DINIZ
CÉSAR DE ARAÚJO GALVÃO
CLAUDIO PICANÇO DA SILVA JÚNIOR
CRISTOFER DIEGO BERALDI MARTINS
EDNA MÁRCIA XAVIER
ELY JOSÉ DE AGUIAR
FARID BUITRAGO SÁNCHEZ
FLÁVIA VIEIRA GUIMARÃES HARTMANN
GABRIELLA DE OLIVEIRA RIBEIRO
GETÚLIO BERNARDO MORATO FILHO
GUSTAVO DE ALMEIDA
IVAN DE FARIA MALHEIROS
JOSÉ FLÁVIO DE SOUZA BEZERRA
JOSÉ NAVA RODRIGUES NETO
JOSIERTON CRUZ BEZERRA
JURACY BARBOSA DOS SANTOS
KENICASSIO JESUS BATISTA
LEONARDO SANTOS ROCHA PITTA
LEONEL ROSSETTI CALVANO
LUIS PIVA JÚNIOR
LUIZ HAMILTON DA SILVA
MARCELA A. MONTANDON GONÇALVES
MARCELLO OLIVEIRA BARBOSA
MÁRCIO ALMEIDA PAES
MARCOS MOURA SANTOS
MÁRIO EUNIDES J. GUIMARÃES JÚNIOR
MIRIAN MINOTTO MARQUES
ODÉSIO LUIZ LUNZ
OSÓRIO LUIS RANGEL DE ALMEIDA
PROCÓPIO MIGUEL DOS SANTOS
RENATA NAYARA DA SILVA FIGUEIREDO
ROSYLANE NASCIMENTO DAS M. ROCHA
SALVADOR CELSO VARELLA ALBUQUERQUE
SÉRGIO TAMURA
TIAGO SOUSA NEIVA
UBIRAJARA J. P. DE MIRANDA JÚNIOR
ULYSSES RODRIGUES DE CASTRO
ZILDINAI FRANÇA DE OLIVEIRA

SUMÁRIO

INTRODUÇÃO

Depois do Marco Civil da Internet, a nova Lei Geral de Proteção de Dados (LGPD) é, seguramente, o maior avanço legislativo brasileiro em termos de proteção da informação que circula na web.

A LGPD surgiu para garantir maior segurança jurídica às atividades de tratamento de dados pessoais no País, estipulando uma série de obrigações para empresas e organizações sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, tanto online quanto offline.

Para os médicos também se aplica a lei, embora já esteja consignado no Código de Ética Médica (CEM) a responsabilidade de proteção aos dados dos pacientes; Diz assim o princípio fundamental número XI do CEM – "*O médico guardará sigilo a respeito das informações de que detenha conhecimento no desempenho de suas funções, com exceção dos casos previstos em lei.*" Posteriormente no capítulo IX do código de ética médica, fica mais explicito todas as obrigações do médico com o Sigilo professional.

Os avanços em tecnologia são inegáveis e a medicina está sempre na vanguarda destes avanços, por tanto muitas das informações médicas são armazenadas em formato digital e é obrigação dos médicos e das empresas o bom uso e guarda destas informações. As empresas que usam o ambiente digital para fazer suas atividades (prontuários, laudos etc.) deverão se ajustar ao que diz a nova lei. Isso porque ela afeta diretamente a forma como os dados de usuários são coletados e tratados, inclusive com sanções para quem descumprir as regras.

O manual de LGPD elaborado pelo CRM-DF busca dar uma orientação aos professionais médicos sobre o manejo das informações e seu ajuste a nova Lei.

1. O QUE É A LGPD?

A Lei Geral de Proteção de Dados Pessoais, nº 13.709, de 14 de agosto de 2018, instituiu um regime geral de proteção de dados no ordenamento brasileiro, a partir de um conceito amplo de dado pessoal e do seu tratamento, submetendo todos os dados pessoais ao seu regime de tutela.

A lei visa proteger os direitos fundamentais de liberdade e privacidade; e se aplica a qualquer pessoa, natural ou jurídica, de direito público ou privado, que realize o tratamento de dados pessoais, no meio físico ou eletrônico.

De acordo com a LGPD, o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

2. CONCEITOS DA LGPD

DADO PESSOAL:

É a informação relacionada a pessoa natural identificada ou identificável; como nome; sobrenome; data de nascimento; número de RG, CPF, e outros documentos pessoais; endereços residencial, comercial e eletrônico; números de telefone.

DADO PESSOAL SENSÍVEL:

É o 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; Nos serviços de saúde, são considerados dados sensíveis as informações acerca de doenças, deficiências, relatórios médicos, prontuários, dados biométricos, resultados de exames, entre outros.

DADO ANONIMIZADO:

dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Os dados anonimizados não são protegidos pela LGPD, uma vez que não são relacionados a titulares específicos.

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 que são objeto de tratamento;

TRATAMENTO:

toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição,

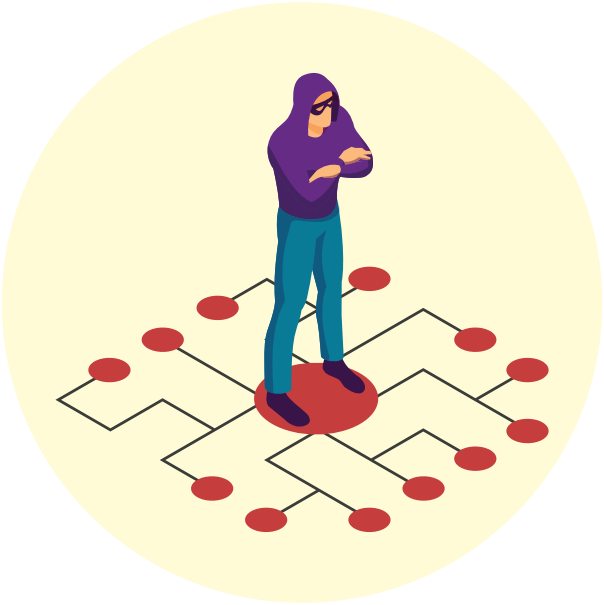
processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

CONSENTIMENTO:

manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

ELIMINAÇÃO:

exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.



3. TUTELA DA SAÚDE

A tutela da saúde é uma das bases legais que autorizam o tratamento de dados pessoais. Apesar disso, o atendimento de saúde deve sempre priorizar o consentimento do paciente; com a oferta de uma escolha real ao titular, sem ser apresentado como uma opção pré-preenchida, devendo ser oferecida uma forma de escolha efetiva, separada dos termos e condições.

Cada termo de consentimento deve ser individualizado, e deve especificar o tratamento a ser feito, bem como, quais os dados dos pacientes serão armazenados pelo profissional. Ademais, deve estar claro que o titular pode corrigir seus dados, e retirar o consentimento quando lhe for conveniente, devendo ser fornecidos os instrumentos para que possa retirar este consentimento de forma simples e facilitada.

Os prestadores de serviços médicos devem ter especial atenção com o PRONTUÁRIO MÉDICO, haja vista ser um documento que contem relevantes dados pessoais e sensíveis do paciente.

O Conselho Federal de Medicina, por meio da Resolução nº 1.605/2000, já determinava o sigilo do prontuário e da ficha médica do paciente, e o desrespeito ao sigilo médico é uma grave infração ética:

Art. 1º - O médico não pode, sem o consentimento do paciente, revelar o conteúdo do prontuário ou ficha médica.

A LGPD reforça a proteção dos dados pessoais já determinadas pelo CFM, e prevê sanções administrativas que podem ser aplicadas independentemente da apuração da infração ética pelo Conselho Regional de Medicina:

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

VII - (VETADO);

VIII - (VETADO);

IX - (VETADO);

X - (VETADO);

XI - (VETADO);

XII - (VETADO);

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Além do prontuário médico, existem outros momentos em que dados pessoais, inclusive sensíveis, são tratados durante a passagem de pacientes pelos estabelecimentos de saúde: no cadastro em clínicas e hospitais; no momento da realização de exames laboratoriais e de imagem; no compartilhamento de exames entre laboratório e hospital; nas consultas e procedimentos médicos; no atendimento via telemedicina.

4. DADOS CADASTRAIS

Nesta etapa da coleta de dados pessoais, é realizado o registro do paciente no estabelecimento de saúde, e devem ser requeridos apenas os dados estritamente necessários para a finalidade pretendida, e se possível, não deve abranger os dados referentes à saúde do paciente.

5. CONSULTA E PRONTUÁRIO MÉDICO

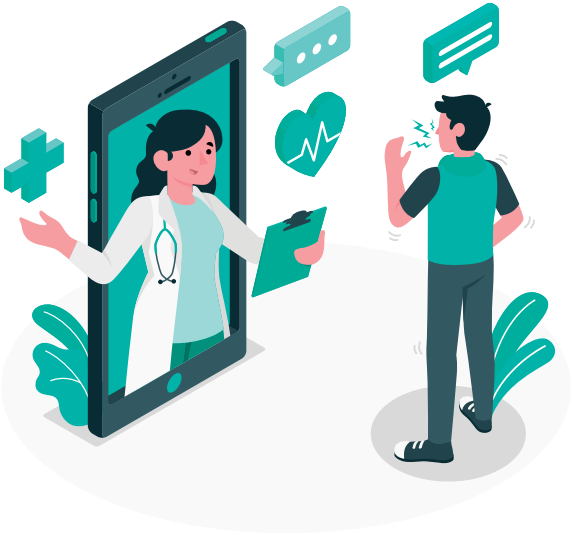
No momento do atendimento médico, naturalmente são coletados os dados sensíveis relativos à saúde do paciente. Além do dever de proteção dos dados pessoais, deve ser resguardado o sigilo médico previsto na Lei nº 13.787/2018 e no Código de Ética Médico.

A Resolução do CFM nº 1638/02 define o prontuário médico em seu art. 1º como "*o conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo*".

Deste modo, devem ser observados:

a) O acesso e manuseio das informações do prontuário médico seja restrito a profissionais de saúde envolvidos no tratamento do paciente que são obrigados ao sigilo profissional;
b) Restringir o acesso e manuseio das informações do prontuário médico a profissionais não obrigados ao sigilo profissional;
c) Cuidado na guarda dos prontuários por terceiros.

6. TELEMEDICINA



As atividades da telemedicina são muito similares às da medicina tradicional, tendo como diferença o fato de o profissional de saúde e o paciente estarem fisicamente distantes. Nesse sentido, deve ser garantida a segurança com os dados dos pacientes e os procedimentos virtuais não podem expor os dados sensíveis dos titulares.

Os médicos devem priorizar a utilização de plataformas digitais que prezem pela segurança e confidencialidade dos dados tratados durante o atendimento, com garantia de acesso individualizado e certificação dos dados, bem como utilizar a assinatura digital.

7. PRESCRIÇÃO ELETRÔNICA

A Resolução CFM Nº 2.299/2021 regulamenta a emissão de documentos médicos eletrônicos, e autoriza a emissão de Prescrição; Atestado; Relatório; Solicitação de exames; Laudo e Parecer Técnico de forma eletrônica, tanto em atendimentos presenciais, como à distância; desde que contenham os seguintes dados:

a) Identificação do médico: nome, CRM e endereço;
b) Registro de Qualificação de Especialista (RQE), em caso de vinculação com especialidade ou área de atuação;
c) Identificação do paciente: nome e número do documento legal;
d) Data e hora;
e) Assinatura digital do médico.

Na emissão de documentos eletrônicos, deve ser assegurado o cumprimento integral à Lei Geral de Proteção de Dados (LGPD), sob pena de responsabilização do médico que realizou o atendimento. Nos estabelecimentos de saúde, a responsabilidade é compartilhada com o diretor técnico das instituições e/ou da plataforma eletrônica.

8. COMPARTILHAMENTO DE INFORMAÇÕES ENTRE OS PROFISSIONAIS DE SAÚDE

As discussões por meio de aplicativos de mensagens, acerca de diagnósticos de pacientes, deve ter a participação APENAS de médicos registrados nos Conselhos de Medicina, e sem referência a casos clínicos identificáveis, e sem exibição de seus pacientes, mesmo com autorização do titular.

Durante o tratamento de saúde, diversos agentes são envolvidos, como médicos, hospitais, laboratórios e plano de saúde, o que gera o compartilhamento de dados sensíveis, e, portanto, todos devem cumprir os requisitos da LGPD.

O compartilhamento dos dados deve sempre ser precedido do consentimento do paciente, e feito exclusivamente em prol da sua saúde, para a realização de procedimentos ou análises em benefício do titular.

No caso de utilização de empresas de tecnologia para gestão de dados dos pacientes, também é necessário o consentimento do titular, para que seja informado de que os seus dados estarão registrados em uma plataforma virtual de saúde.

O profissional de saúde deve avaliar

os riscos na utilização das plataformas virtuais, com controles de acesso; bem como garantir a segurança da utilização de wi-fi, ethernet, bluetooth, USB, e outros.

9. CONSIDERAÇÕES FINAIS

O setor de saúde conta com grande utilização de dados sensíveis dos pacientes, e por essa razão, devem ser adotados procedimentos que garantam a privacidade dos titulares de dados.

As instituições de saúde deverão se adequar a fim de se prevenirem em relação às sanções por vazamentos de dados de pacientes, ataques hackers e falha humana decorrente da atuação de seus funcionários que tiverem acesso aos dados de pacientes.

Cada estabelecimento de saúde deve criar diretrizes para assegurar a proteção dos dados pessoais. Assim, apenas pessoas autorizadas devem ter acesso a dados dos pacientes, e, em caso de desligamento, a imediata revogação das autorizações. Devem ser protegidos os logins de acesso, e, se possível, ser adotado um segundo fator de autenticação.

As informações armazenadas em quaisquer meios, sejam físicos ou digitais, devem contar com proteção, por meio de registros de data, hora, duração e identidade do responsável pelo acesso e ações executadas; bem como com soluções de proteção e segurança, com redes criptografadas e softwares de monitoramento.

CONSELHO REGIONAL DE MEDICINA DO DISTRITO FEDERAL