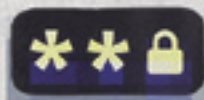


O SETOR DA SAÚDE E A **LEI GERAL DE PROTEÇÃO DE DADOS**



SUMÁRIO

1. O que é a Lei Geral de Proteção de Dados (LGPD)?
2. A quem a LGPD se aplica?
3. Qual a diferença entre dado pessoal e dado pessoal sensível de saúde?
4. Qual a finalidade da LGPD para o Setor de Saúde?
5. Em quais situações a área da saúde utiliza dados pessoais?
6. É sempre necessário consentimento do paciente para o tratamento de dados de saúde?
7. Por que a área da saúde precisa estar atenta à LGPD?
8. Como proteger meus dados pessoais de saúde?
9. Como adequar os serviços e instituições de Saúde à LGPD?



O QUE É A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)?

Privacidade e proteção de dados são assuntos que estão em alta no mundo inteiro nos últimos anos. Atualmente, vivemos na chamada “Era dos Dados” ou “Sociedade da Informação”, que estabeleceu um inegável confronto entre o controle e a proteção de dados pessoais dos cidadãos.

Hoje estamos todos hiperconectados, coletando e fornecendo uma quantidade enorme de dados pessoais, processados e armazenados por sistemas computacionais como redes sociais, gerenciadores de e-mails, sistemas financeiros e também aplicativos.

Em razão disso, diversas legislações vêm sendo debatidas e criadas nos países com a finalidade de fiscalizar essa troca de informações que ocorre constantemente e até mesmo inconscientemente entre os usuários.

Como resultado, observamos que os titulares dos dados estão cada vez mais preocupados com a sua privacidade e que as empresas, Instituições e profissionais estão cada vez mais zelosos com os dados pessoais dos seus clientes, entendendo essa área como uma forma de se diferenciar no mercado.

No Brasil, a Lei Geral de Proteção de Dados (Lei nº. 13.709/2018), que entrou em vigor no ano de 2020, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

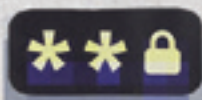
A QUEM A LGPD SE APLICA?

A LGPD é aplicável a todas as pessoas naturais e jurídicas, de direito público ou privado, independentemente do meio, do país de sua sede ou do país em que estejam localizados os dados, desde que:

- a) O tratamento de dados seja realizado no Brasil;
- b) Os dados tenham sido coletados no território nacional; ou
- c) Ainda que ausente alguma das situações anteriormente descritas, o tratamento tenha por objetivo a oferta ou fornecimento de bens ou serviços a indivíduos localizados no país.

Por outro lado, a LGPD NÃO se aplica ao tratamento de dados realizado:

- a) Por pessoa natural para fins exclusivamente particulares e não econômicos (ex: lista de festa de aniversário);
- b) Para fins exclusivamente jornalísticos, artísticos e acadêmicos;
- c) Para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais;
- d) Quando os dados sejam provenientes de países que, por sua vez, ofereçam um nível de segurança jurídica adequado sobre esse assunto e apenas processados em território nacional, sem que haja qualquer intenção do agente brasileiro em compartilhar ou comunicar esses dados pessoais com outros agentes, exceto o agente que primariamente transmitiu a informação.



QUAL A DIFERENÇA ENTRE DADO PESSOAL E DADO PESSOAL SENSÍVEL DE SAÚDE?

Para a LGPD, dado pessoal é qualquer dado que identifique (nome, RG, CPF) ou que possa identificar o seu titular (perfil comportamental, número identificador do seu celular e IP).

Os dados pessoais sensíveis dizem respeito a uma parte muito íntima da pessoa e, em virtude desta característica, podem gerar discriminação. Assim, esses dados precisam de um tratamento distinto e de uma maior atenção.

Nesse sentido, são dados pessoais sensíveis: origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou 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.

O Setor de Saúde lida diariamente com um conjunto enorme de dados sensíveis de pacientes. Assim, toda informação, seja de natureza diagnóstica ou terapêutica, desde que colhida nesses contextos, são consideradas dados sensíveis de saúde, cabendo aos profissionais e organizações do setor zelar pelos dados de seus pacientes e buscar a conformidade necessária para o adequado tratamento desses dados.

QUAL A FINALIDADE DA LGPD PARA O SETOR DE SAÚDE?

A LGPD tem a finalidade de proporcionar maior segurança informacional em relação aos dados pessoais dos cidadãos.

Como mencionado, o Setor de Saúde é um dos setores que mais tratam dados considerados sensíveis pela nova legislação. Isso porque há todo um ecossistema interligado, que pode ir desde a clínica médica até o hospital, laboratório, farmácia, o paciente e os agentes de saúde.

E é justamente em razão desse grande volume de dados pessoais sensíveis tratados, que o setor também atrai grandes riscos e atenção.

Dessa forma, é imprescindível, tanto para garantir a segurança dos titulares dos dados, como para garantir a segurança e eficiência do trabalho realizado pelo Setor de Saúde, estar adequado à legislação de proteção de dados.

As organizações de saúde precisam, portanto, investir para mudar sua perspectiva e abordagem, já que para estar em conformidade com a nova regulamentação de proteção de dados pessoais é essencial aplicar melhores práticas de cibersegurança, por exemplo.

O setor de saúde, juntamente com muitos outros, está se tornando cada vez mais dependente de dados e análises para fornecer serviços mais rápidos e melhores. É um dos setores que passam por grande inovação e transformação digital, já com uso de IA, Big Data, machine learning, plataformas em nuvem e tudo mais. Por isso, o cumprimento da regulamentação de proteção de dados é uma responsabilidade que ultrapassa os limites geográficos, especialmente para um setor que lida com a segurança física e emocional dos indivíduos.

EM QUAIS SITUAÇÕES A ÁREA DA SAÚDE UTILIZA DADOS PESSOAIS?

Nos dias atuais, praticamente todos os setores tratam dados pessoais no exercício de suas atividades, havendo a necessidade de se atentar para o tema da proteção de dados e LGPD.

Como já mencionado, o Setor de Saúde é um dos setores que mais tratam dados considerados sensíveis pela nova legislação, já que a própria LGPD considera todos os dados de saúde e genéticos sensíveis, demandando uma maior atenção (art. 5º, II, LGPD).

Nesse sentido, citamos alguns exemplos específicos de dados pessoais tratados no Setor de Saúde:

- Atendimento de pacientes (fichas cadastrais, etc.);
- Hospitais (cadastros, prontuários médicos, dados relacionados a cirurgias e procedimentos, etc.);
- Laboratórios (cadastros, resultados de exames, procedimentos, medicamentos);
- Clínicas e consultórios médicos (assim como o hospital, cadastros, prontuários médicos, dados relacionados a cirurgias e procedimentos, etc.);
- Telemedicina (cadastros, dados sobre a saúde do paciente, resultados de exames, prescrição de medicamentos, etc.);
- Farmácias (cadastros, perfil farmacoterapêutico do titular, etc.);
- Precificação de plano e dos serviços de saúde: Segundo o art. 9º, da RN 162, da ANS, para a contratação de qualquer plano de saúde, o contratante deve apresentar a chamada Declaração Pessoal de Saúde (DPS), por meio da qual deverá informar sua condição atual de saúde e eventuais doenças pré-existentes para que a operadora possa então verificar a necessidade de aplicação de Carência, Agravo ou Cobertura Parcial Temporária. Todas essas informações são dados pessoais, podendo também constar dados pessoais sensíveis.

É SEMPRE NECESSÁRIO O CONSENTIMENTO DO PACIENTE PARA O TRATAMENTO DE DADOS DE SAÚDE?

A regra geral é a de vedação do tratamento de dados pessoais sem o expresso consentimento do paciente ou de seu responsável, sendo assim, o profissional e/ou organização deve formalizar por escrito o Termo de Consentimento Informacional a fim de se evitar erros e vícios da manifestação de vontade.

Contudo, com o objetivo de não inviabilizar a assistência à saúde por falta de assinatura de documentos, a Lei determinou exceções à obrigatoriedade da obtenção do consentimento. Podendo esse ser dispensado em relação aos dados pessoais sensíveis para a Tutela da Saúde do titular, exclusivamente, em procedimento realizado pelos profissionais de saúde, serviços de saúde ou autoridade sanitária.

O termo Tutela da Saúde incorporado pela Lei é extremamente indeterminado. Neste caso, podemos recorrer à visão assistencial de definições de Urgência e Emergência, contidas na Resolução do Conselho Federal de Medicina (CFM) n. 1.451, de 1995. Isso significa dizer que, no âmbito da assistência em saúde, a assinatura do Termo de Consentimento pelo paciente para o tratamento de seus dados pessoais de saúde não é essencial à prestação do serviço.

Do ponto de vista constitucional e da própria LGPD, o direito à vida e à integridade física sobrepõe-se à vontade do titular consentir ou não. Logo, o profissional possui o dever de prestar a assistência, independentemente da assinatura do termo de consentimento informacional. Contudo, nesses casos, recomenda-se fortemente fazer constar por escrito nos registros e prontuários a impossibilidade da obtenção do consentimento.

POR QUE O SETOR DA SAÚDE PRECISA ESTAR ATENTO À LGPD?

O setor da Saúde é sem dúvidas o que mais trata dados pessoais considerados sensíveis pela nova Lei Geral de Proteção de Dados Pessoais e, inevitavelmente, trará grandes desafios aos profissionais e organizações de saúde. A Lei já está em vigor desde agosto de 2020 e chega em uma época propícia, marcada por grandes vazamentos de informações e escândalos que envolvem o uso indevido de informações pessoais de saúde.

O tratamento de dados pessoais de saúde apresenta elevado índice de risco jurídico, isso porque são informações da esfera mais íntima de uma pessoa e sua exposição inadequada pode causar danos irreversíveis de ordem moral e patrimonial, gerando responsabilização e o consequente dever de indenizar em caso de vazamento ou uso indevido.



COMO PROTEGER MEUS DADOS PESSOAIS DE SAÚDE?

- Se possível, busque atendimento em instituições de saúde que possuam um sólido Programa de Privacidade e Proteção de Dados.
- Certifique-se que os dados fornecidos durante uma consulta de telemedicina estão protegidos para evitar acesso não autorizado, por meio de medidas de segurança da informação apropriadas.
- Proteja sua máquina de ataques virtuais. Mantenha antivírus e firewalls atualizados, e procure navegar e fazer downloads via sites confiáveis.
- Se não quiser receber e-mails com propagandas, lembre-se que, com a LGPD, as empresas só poderão enviar publicidade se você der o consentimento prévio; e, caso você autorize, deverão oferecer a você a opção de sair da lista de envios.
- Escolha suas senhas cuidadosamente. Faça senhas fortes, que não sejam fáceis de serem desvendadas por terceiros.
- Deixe sua conexão Wi-Fi mais segura com pequenas atitudes: não deixe o nome de fábrica, troque; desative a conexão automática, porque assim você não corre o risco de ser conectado automaticamente a redes abertas desconhecidas e potencialmente perigosas.
- Não disponibilize suas informações de saúde a qualquer pessoa, como em cadastros físicos ou on-line.
- Ative a criptografia nos discos e mídias externas, como pendrives e crie senhas fortes, que contenham a combinação de caracteres especiais, letras maiúsculas, minúsculas e números, evitando utilizar dados pessoais ou palavras comuns;
- Ative a criptografia nos discos e mídias externas, como pendrives e crie senhas fortes, que contenham a combinação de caracteres especiais, letras maiúsculas, minúsculas e números, evitando utilizar dados pessoais ou palavras comuns;
- Habilite a verificação de senhas em duas etapas, sempre que disponível, principalmente em sistemas de armazenamento em nuvem e

- Ative a criptografia nos discos e mídias externas, como pendrives e crie senhas fortes, que contenham a combinação de caracteres especiais, letras maiúsculas, minúsculas e números, evitando utilizar dados pessoais ou palavras comuns;
- Habilite a verificação de senhas em duas etapas, sempre que disponível, principalmente em sistemas de armazenamento em nuvem e aplicativos de mensagens;
- Instale somente aplicativos de fontes e serviços oficiais;
- Atualize sempre o sistema operacional e os aplicativos;
- Apague os dados pessoais de saúde armazenados antes de se desfazer dos equipamentos e das mídias;
- Desconfie de links recebidos por aplicativos de mensagens;
- Limite a divulgação ou fornecimento de dados pessoais de saúde na internet, inclusive para redes sociais, ou para empresas, aos casos estritamente necessários;



COMO ADEQUAR OS SERVIÇOS E INSTITUIÇÕES DE SAÚDE À LGPD?

As instituições de saúde possuem grandes desafios pela frente: adequar a documentação médica e institucional, implementar políticas de governança, garantir certificação de segurança para os softwares e aplicativos que contenham informações de pacientes e providenciar que todas as informações de bancos de dados, transmissões ou transações digitais, sejam criptografadas.

A LGPD exige que as organizações tenham uma política clara e transparente para a coleta e tratamento de dados. É necessário realizar ações de revisão e adequação, devendo estar incluídas no conjunto de políticas aquelas de segurança da informação, de privacidade, de classificação da informação e de controle de acesso, devendo essas serem amplamente divulgadas para seus colaboradores e, também, para os pacientes.

Para tal, as instituições devem contar com assessoria jurídica especializada em saúde, promover auditoria interna com especialistas em segurança da informação e investir na implementação de serviços com tecnologia de ponta. Sempre com o objetivo de verificar o que está, ou não, em conformidade com a lei. Garantindo de fato a segurança dos dados dos pacientes e, conseqüentemente, protegendo a reputação da instituição.

Neste sentido, os colaboradores da instituição devem ser instruídos a assinar um Termo de Responsabilidade para que, em caso de incidente, não venham a alegar desconhecimento das normas e procedimentos de segurança da informação do ambiente hospitalar e certificar que os fornecedores de softwares e bancos de dados e provedor de hospedagem, por exemplo, também estejam adequados às novas regras.

A principal característica positiva da lei é a mudança cultural do atual tratamento de dados pessoais no Brasil. A LGPD provê maior segurança jurídica e fomenta boas práticas empresariais, regulando as relações entre setores da economia, poder público e seus usuários. O objetivo é atribuir maior proteção à parte mais vulnerável da relação, o consumidor de bens e serviços. Os profissionais e empresas que se adequarem certamente estarão na vanguarda do desenvolvimento econômico e cultural, além de prevenirem possíveis demandas judiciais.



Cuiabá (MT), janeiro de 202



Tassia Neumann Hammes Haddad
Priscila Mendonça de Aguiar Arruda