ASPECTOS PRÁTICOS DA **LGPD | LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS** | PARA MÉDICOS E CLÍNICAS

SINMED | MG
SINDICATO DOS MÉDICOS DE MINAS GERAIS | JUNTOS SOMOS MAIS FORTES

INTRODUÇÃO

O Sindicato dos Médicos de Minas Gerais, por meio de escritório de advocacia parceiro, produz essa cartilha com o objetivo de orientar os médicos acerca de um tema atual muito importante para a categoria: a **Lei Geral de Proteção de Dados Pessoais (LGPD)**.

Importantes orientações como as determinações da LGPD nos serviços de saúde, as obrigações impostas e as penalidades para descumprimento da lei, além de informações úteis para os médicos sobre o tema estarão presentes nessa cartilha.

Na área da saúde, especialmente no Direito Médico, o tema da segurança das informações é bastante relevante e mesmo que os dados processados por uma instituição de saúde, seja um grande hospital ou um consultório, já estejam protegidos pelo segredo da profissão médica, e já gozavam de confidencialidade e proteção, a LGPD reforça esse comando, informando claramente sua sensibilidade e critérios para o processamento.

Destacamos que o Sinmed-MG conta com uma equipe especializada de advogados parceiros, prontos para orientar você e garantir seus direitos. Conte com o seu sindicato!

1 | O QUE DETERMINA A LGPD NO QUE DIZ RESPEITO AOS SERVIÇOS DE SAÚDE?

A Lei Geral de Proteção de Dados não inova em obrigações para o mercado de saúde. Critérios de segurança e confidencialidade trazidos pela lei fazem parte do cotidiano dos profissionais que recebem, diariamente, informações sobre saúde e da vida privada de seus pacientes.

Se é assim, por que a LGPD deve ser preocupação para os profissionais da saúde?

A lei 13.709, publicada em 2018 e vigente desde setembro de 2020, estabelece parâmetros e atenção para o uso seguro de informações pessoais confiadas a empresas e profissionais liberais que, no exercício de suas atividades, processam tais dados.

A nova lei também nos aproxima de conceitos como “titulares”, “controladores” e “operadores”, definindo direitos, obrigações e responsabilidade conjunta (solidária) entre os dois últimos, em atenção à eventual violação da privacidade dos dados pessoais do primeiro, definindo de forma clara sanções administrativas e a possibilidade de ações judiciais de reparação de dano.

Ou seja, a **LGPD define critérios para o processamento seguro de informações pessoais**, obrigando aqueles que recebem os dados em confiança a tratá-los adequadamente, sob pena de serem responsabilizados e punidos quando deixarem de observar as melhores práticas de governança de dados e atenderem às expectativas de documentação e controle definidos pela legislação.

Na Saúde a LGPD é ainda mais exigente e rigorosa. Isso se deve à sensibilidade das informações pessoais processadas neste segmento. A nova lei informa que são sensíveis os dados que identificam ou tornam alguém identificável e que tenham a capacidade de trazer prejuízos (como limitação de acesso a bens e serviços, discriminação, etc). No rol destes dados sensíveis o legislador incluiu, entre outros, os dados referentes à saúde.

Os dados processados por uma instituição de saúde, seja um grande hospital ou um consultório, estão protegidos pelo segredo da profissão médica, e já gozavam de confidencialidade e proteção. A LGPD reforça esse comando, informando claramente sua sensibilidade e critérios para o processamento.

2 | QUAIS AS OBRIGAÇÕES IMPOSTAS E PENALIDADES POR DESCUMPRIMENTO DA LEI?

O legislador, ao editar a Lei Geral de Proteção de Dados, foi muito assertivo ao estabelecer fundamentos e princípios para o processamento de dados pessoais.

Entre os fundamentos da lei, temos o **respeito à privacidade**, como um forte indicativo do que se espera do comportamento das instituições e pessoas que processam dados pessoais.

Na sequência temos a **autodeterminação informativa** para permitir que o titular de dados, que empresta suas informações para um processamento, o faça consciente de todas as tratativas e uso que aquela informação servirá.

Continua a lei estabelecendo ainda a l**iberdade de expressão, de informação, de comunicação e de opinião**, bem como a **inviolabilidade da intimidade, da honra e da imagem**.

Nesse caminho, a lei mantém seu caráter orientador ao informar como fundamentos o **desenvolvimento econômico e tecnológico**, bem como a **inovação**, e ainda, a l**ivre iniciativa, livre concorrência e a defesa do consumidor**.

Por fim, mas igualmente relevante, temos os **direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania**.

Esses são os fundamentos da LGPD. Devem ser observados como obrigação por aquele que recebe os dados em confiança, antes mesmo de qualquer processamento. O uso de dados pessoais em ações que sejam conflitantes com esses fundamentos indicará que o processamento é inadequado e sujeito às sanções da legislação.

Assim como os fundamentos devem ser orientadores da conduta, também temos os princípios. Ao definir os princípios, o legislador foi bastante didático, explicando cada ponto:

- Finalidade | realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- Adequação | compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- Necessidade | limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- Livre acesso | garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- Qualidade dos dados | garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- Transparência | garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

- **Segurança** | utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- **Prevenção** | adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- **Não discriminação** | impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- **Responsabilização e prestação de contas** | demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Os desdobramentos da LGPD para o processamento de dados podem ser simplificados em tratar apenas o que for necessário para uma finalidade específica, adequada a uma alinhamento de processos, de forma segura e com prevenção, prestigiando a transparência, sem causar qualquer tipo de dano ao titular, sob pena de sanções administrativas e outras consequências.

As sanções podem variar de simples advertência à exclusão do banco de dados, passando por multas, multas diárias e publicização das ocorrências de violação de dados e vazamentos.

3 | QUAIS OS TIPOS DE CUIDADOS A SEREM TOMADOS PELOS MÉDICOS E A PARTIR DE QUANDO?

A LGPD está vigente desde o dia 18 de setembro de 2020. Logo, suas obrigações são exigíveis desde então. Em agosto de 2021 entrarão em vigor as sanções administrativas, mas sua ausência momentânea não exime os hospitais, as clínicas e os profissionais liberais em seus consultórios das obrigações quanto a documentação, o controle, a segurança da informação e o atendimento aos titulares em relação aos seus direitos.

Assim, deve o profissional se resguardar, revisando seus processos e identificando quais são as informações que de fato são úteis ao processamento, eliminando excessos e revisando rotinas para tratar adequadamente as informações.

Ao fazer uso de prontuários eletrônicos, é recomendável avaliar se os requisitos mínimos de segurança foram empregados quanto à confidencialidade, integridade e disponibilidade das informações. Ou seja, o sistema deve ser capaz de proteger as informações de acessos indevidos, alterações sem referência ou autorização e a manutenção da informação disponível.

Se o armazenamento for em "nuvens", deve o profissional ter a segurança do local do processamento das informações, especialmente quando se tratar de hospedagem internacional. Lembrando que a LGPD possui restrições para o processamento de dados pessoais em países sem legislação semelhante.

Também é importante **capacitar e garantir a compreensão dos funcionários e parceiros quanto à confidencialidade das informações acessadas**. Recomenda-se repetir o treinamento a cada período e atualizar os termos de confidencialidade e ciência.

Neste sentido é indispensável estabelecer políticas e normas de segurança que contribuam para a mudança de cultura e para a incorporação de conceitos tecnológicos de proteção de dados, como o uso de antivírus, firewall e proteções de rede e monitoramento de acesso.

Além disso, deve existir uma atenção especial ao titular dos dados, garantindo que todas as informações quanto ao processamento de dados lhe sejam prestadas, e quando necessário, seu consentimento seja colhido e gerenciado.

Também é importante destacar a necessidade de gerenciar todas as fases desse processo de transformação, documentando as ações e as alterações de rotinas e controles. A propósito, a LGPD estabelece dois relatórios obrigatórios. O Relatório Geral de Processamento e o Relatório de Impacto à Proteção de Dados.

4 | QUAL A FORMA CORRETA DE CUIDAR DOS DADOS PESSOAIS DOS PACIENTES E FUNCIONÁRIOS?

A Lei Geral de Proteção de Dados Pessoais impõe obrigações a quem realiza tratamento de dados de titulares, recebidos em confiança. Esse tratamento deve observar os princípios da necessidade, adequação e finalidade. Ou seja, **somente podem ser processados dados necessários, alinhados a um objetivo específico e com um propósito justo pré-determinado**.

Esse processamento deverá ser seguro, transparente, não discriminatório, sob pena de responsabilidade de quem deixar de observar tais critérios. Assim, o legislador definiu como deve ser o cuidado com os dados pessoais.

Não obstante aos princípios, o legislador insistiu em detalhar as possibilidades para o tratamento, começando pelo consentimento e detalhando outras nove hipóteses, cada uma com sua reserva, condição e limitação, especialmente para dados sensíveis.

As chamadas bases legais delimitam o processamento e orientam a conduta quanto ao tratamento a ser dado cada a caso.

Também é importante destacar que a nova lei define os critérios de segurança e de notificação de incidentes de segurança como um protocolo obrigatório. Além disso, preserva os conceitos de segurança da informação como requisitos para manutenção da privacidade de pessoas, devendo ser observados em todas as fases do tratamento, desde o início, por padrão.

Por fim, a LGPD estabelece a necessidade de um pensamento voltado para controle e gestão da informação, que determina a manutenção de um programa de governança, com revisão e atualização contínua, foco e controle, garantindo a evolução da segurança e aprimoramento do pensamento e cultura orientados pela privacidade, independente se dados de pacientes, funcionários, parceiros ou prestadores de serviço.

5 | QUAIS SÃO OS CUIDADOS ESPECIAIS COM DADOS DE MENORES DE 18 ANOS?

Ao definir as bases legais, a LGPD elenca 10 opções pelas quais é possível o tratamento de dados pessoais. Contudo, estabelece que o tratamento de **dados pessoais de crianças e adolescentes, ou seja, menores de 18 anos, somente podem ser processados com o consentimento dos pais ou responsáveis**, ou para a proteção da própria criança, para contatar os pais, sem autorização de armazenamento.

Tal condição já é conhecida e praticada por instituições e profissionais, mas em alguns casos há falta de controle objetivo quanto a aplicação, o que agora exigirá atenção.

Para tratamento de dados de crianças e adolescentes é necessário consentimento. E este deve ser gerenciado de forma a garantir o cumprimento do que é necessário para o atendimento ao menor, pelo tempo legal e com a segurança adequada para instituições e profissionais.

6 | QUANDO OS DADOS DE SAÚDE PODEM SER COMPARTILHADOS, EM QUAIS HIPÓTESES E CONDIÇÕES?

Dados pessoais confiados para tratamento podem ser compartilhados, observando critérios de transparência, adequação e necessidade, assim como segurança e alinhamento contratual.

O mesmo se aplica a dados sensíveis, mas com restrições. No caso da saúde, por sua sensibilidade e grande valor mercantil, a LGPD define critérios objetivos e limitantes ao compartilhamento com objetivo de obtenção de vantagem econômica. No caso, qualquer compartilhamento de dados de saúde é vedado pela lei, excetuando as hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde.

Isto é, **práticas de venda ou troca de bancos de dados**, seja com prontuários ou informações que permitam identificar pacientes e suas comorbidades, bem como consumo de medicamentos e hábitos de vida relativos a sua saúde, **são proibidos**. Tal conduta é compreendida como incidente de segurança com violação de dados pessoais, passível de sanções administrativas, cíveis e penais.

7 | E SE HOUVER VAZAMENTO DE DADOS, QUAIS AS RESPONSABILIDADES DO MÉDICO PELO INCIDENTE DE SEGURANÇA?

A LGPD inaugura um novo momento quanto ao controle do uso de informações pessoais, embora não inove em obrigações e responsabilidades. A nova lei, ao definir responsabilidade e sanções, coloca condições de processamento seguro da informação e determina a necessária apresentação de relatórios e notificações para casos de incidentes de segurança e vazamentos.

O vazamento de dados é o pior cenário que pode ocorrer em uma instituição de saúde. Especialmente se este vazamento comprometer dados de pacientes, como prontuários e faturamento. Ou ainda dados de funcionários, como endereço, salários e condições de saúde.

O cenário se agrava se as medidas de contenção não forem suficientes para conter o atacante e este conseguir copiar do ambiente as informações, deixando a instituição com a obrigação de avaliar a sensibilidade e o volume de dados, e conforme o resultado, ter que notificar a autoridade e também aos titulares. Nesses casos, é importante ter um plano de gerenciamento de crise.

Não fosse suficiente a possibilidade das sanções (suspensas até agosto de 2021), ao notificar ao titular, este poderá, conforme seu sentimento e lesão, ajuizar ações para reparação de eventuais danos.

O profissional médico que recebe os dados em confiança deverá, a qualquer medida de segurança e controle, garantir que as informações estejam seguras e monitoradas. E quando arquivadas, física ou digitalmente, **sejam criptografadas**, de forma a limitar o acesso e o interesse do atacante às informações. Não tomar ações de proteção significa correr riscos em um ambiente digital voraz e ansioso pela primeira oportunidade.

8 | MEDIDAS DE ENFRENTAMENTO POR MÉDICOS E EQUIPES CLÍNICAS PARA A REDUÇÃO DOS RISCOS NO TRATAMENTO DE DADOS?

Os primeiros passos para a conformidade LGPD são tomados no sentido de identificar o cenário atual de uso de dados e de proteção oferecida, com a escrituração de robusto diagnóstico, levantamento de processo e avaliação de riscos.

Uma vez identificado o cenário, do processo mais crítico para o menos, deve a instituição ou profissional adotar uma das seguintes medidas, conforme avaliação e entendimento institucional:

- Eliminar o risco | Implica em definir ações que eliminem, totalmente, a possibilidade de ocorrência do risco. São ações de enfrentamento da questão, envolvendo ações e investimentos que descartam totalmente a possibilidade do risco ocorrer.
- Mitigar o risco | Aqui temos ações que não eliminam o risco mas o diminuem a um ponto menor ou até mesmo aceitável.
- Transferir o risco | São os casos em que se contrata um seguro, por exemplo, transferindo aquele risco a uma terceira pessoa que será responsabilizada.

- **Aceitar o risco** | Uma das decisões mais difíceis, vez que envolverá um estudo de histórico, causas e consequências. O ato de aceitar o risco implica em assumir responsabilidade por sua ocorrência, o que também exigirá robusta documentação com autorização de toda estrutura gestora da instituição.

Definidas as medidas, estas devem ser postas em prática e monitoradas constantemente. Em especial as ações que diminuam os riscos (mitigadoras) e de aceitação. Apenas o monitoramento será capaz de permitir agir antes da ocorrência, ou ainda no início, minimizando impactos e consequências.

Portanto, um plano de ação e a implantação de protocolos e monitoramento, preferencialmente digital, são indispensáveis para a prevenção de riscos ou, minimamente, seu gerenciamento.

31 3241.2811 31 99302.0097 sinmedmg.org.br @Sinmedmg /sinmedMG @sinmedmg Sinmed-MG Oficial

PARCERIAS

AGILE FOR ALL

COSTA JORGE
SOCIEDADE DE ADVOGADOS

HDPO
Health Data Privacy Office

SISTEMA DE GESTÃO LGPD
PROTEGEON

REALIZAÇÃO

SINMED MG
SINDICATO DOS MÉDICOS DE MINAS GERAIS
JUNTOS SOMOS MAIS FORTES