Mettricx

The Blockcain Company

Saúde 4.0 e a LGPD

LGPD

Estamos desenvolvendo em parceria com um Centro de Reabilitação Físico e Mental um Sistema para automatizar os processos de Consulta médica, estamos então em constante contato com os profissionais, de diversos níveis, desta área. O que chama atenção é o desconhecimento total ou parcial sobre a LGPD e seu impacto na área Médica. Todos entendem a necessidade da confidencialidade de dados segundo a Ética Médica, mas, especificamente sobre a LGPD as coisas mudam de figura. Existe até o questionamento se essa é uma lei que vai "pegar" ou não, mas o fato é que ela existe.
A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) estabelece padrões, regras e princípios para o tratamento de dados pessoais. Clínicas médicas, hospitais e demais estabelecimentos de Saúde têm até **agosto de 2020** para adequar seus processos e sistemas às novas sanções da referida lei. Compartilho neste artigo alguns ítens que achei importante durente o meu processo de entendimento desta Lei.

ANS Nota Técnica Nº 3/2019

A Agência Nacional de Saúde Complementar lançou esta Nota Técnica com o objetivo avaliar as implicações para a ANS e o setor regulado que transacionam dados pessoais. O que será necessário para adequar seus processos às exigências da lei.

Alcance da norma

A LGPD se limita a regular o tratamento de dados pessoais:
a) de pessoas naturais (Pessoa Física).
b) realizados no território brasileiro ou no exterior, se os dados pessoais forem coletados no Brasil, se eles se relacionarem a indivíduos localizados no território brasileiro.

Dados pessoais e dados pessoais sensíveis

O art. 5º, I da LGPD considera dado pessoal a "informação relacionada a pessoa natural identificada ou identificável". Isto é, para ser relevante à privacidade, a informação precisa ser

	pessoal, nominativa, ou seja, ela deve ser coletada de forma individual e não anônima. Dados não personalizados, seja pela agregação em grupos ou categorias, ou, quando individualizados, pelo anonimato, destinados exclusivamente para **fins estatísticos**, não afetam a esfera de intimidade. Entretanto, deve ser observado que mesmo que não haja uma identificação clara, como nome, endereço, mas sim a combinação de atributos, como CEP, profissão e idade por exemplo, talvez seja possível revelar a identidade do indivíduo.
Dados Sensíveis	A LGPD protege com mais rigor os dados pessoais Sensíveis, a saber: "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"**.**
Atores da Proteção de Dados Pessoais	a) **titular** - pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (o Paciente); b) **agentes de tratamento** - o controlador e o operador; c) **controlador** - pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (o Hospital, por exemplo); d) **operador** - pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (a empresa de software); e) **encarregado** - pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); f) **autoridade nacional** - órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.
Tratamento de dados pessoais	Deve haver o expresso **consentimento do titular** ou de seu responsável legal para que os dados pessoais sejam tratados. Esta restrição é estendida a qualquer informação pessoal, não apenas a informações sensíveis
Dispensa do consentimento	As hipóteses de dispensa do consentimento prévio para o tratamento de dados pessoais estão previstas no art. 7º e no art. 11º, II da LGPD. Dentre elas, a mais relevante para a ANS é a referente aos "dados necessários à execução, pela

administração pública, de políticas públicas previstas em leis ou regulamentos" (art. 7º, III, e art. 11, II, “b”). Alguns exemplos:

- ❏ compartilhamento de registros de saúde com os médicos assistentes para melhorar o cuidado e o resultado em saúde para o paciente;
- ❏ utilização de informações de saúde por gestores de sistemas de saúde públicos ou privados para a condução de programas de promoção de saúde e de prevenção de doenças, bem como para o direcionamento dos pacientes para prestadores mais adequados para seus quadros;
- ❏ comunicação à autoridade sanitária de suspeita ou confirmação de doença ou agravo e eventos de saúde pública, como acidentes de trabalho, doenças infecto-contagiosas, violência doméstica etc;

Direitos do titular

O titular tem direito de obter do controlador, mediante requisição:

1. a revogação do consentimento do tratamento de dados, por procedimento gratuito e facilitado;
2. a confirmação da existência de tratamento no prazo de 15 dias;
3. o acesso aos dados em meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa;
4. a correção de dados incompletos, inexatos ou desatualizados;
5. a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD;
6. a 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;
7. a eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 (art. 18, VI);
8. informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados

Obrigações dos agentes de tratamento de dados

1. dar publicidade às informações sobre tratamento de dados;
2. disponibilizar meios de receber, processar e atender às requisições dos titulares de dados pessoais;

3. indicar o encarregado pelo tratamento de dados pessoais;
4. divulgar publicamente a identidade e as informações de contato do encarregado;
5. juntamente com o operador, manter registro das operações de tratamento de dados pessoais que realizarem;
6. quando solicitado pela ANPD, elaborar relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial;
7. juntamente com o operador, adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito, mesmo após o término do tratamento, inclusive adotando sistemas conformados aos requisito de segurança, aos padrões de boas práticas e de governança e aos princípios gerais;
8. previstos na LGPD e às demais normas regulamentares;
9. juntamente com o operador e com qualquer pessoa que intervenha em qualquer fase do tratamento, garantir a segurança da informação prevista na LGPD em relação aos dados pessoais, mesmo após o término do tratamento;
10. no caso de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, comunicar a ocorrência do incidente à ANPD e ao titular e adotar as providências determinadas pela ANPD.

Obrigações específicas

1. Manter os dados pessoais em formato interoperável e estruturado para o uso compartilhado com vistas à execução de políticas públicas, à disseminação e ao acesso das informações pelo público em geral;
2. comunicar à ANPD contratos e convênios celebrados com entidades privadas que envolvam a transferência de dados pessoais constantes de suas bases de dados;
3. informar à ANPD e ao titular a comunicação ou o uso compartilhado de dados pessoais, ressalvadas as exceções previstas na LGPD;

Requisitos para aplicação da LGPD na saúde suplementar

1. Organização e Comunicação

- ❏ Nomear o Oficial de Proteção de Dados (DPO).
- ❏ Identificar as funções da própria organização e dos parceiros: Controladores de Dados / Processadores de dados.
- ❏ Estabelecimento de padrões mínimos para um Projeto de Governança da Informação e Proteção de Dados;
- ❏ Divulgação em veículos de fácil acesso a finalidade, práticas de execução e previsão de tratamento de dados públicos. Indicação de Encarregado da função para tal.
- ❏ Criar novo aviso de privacidade e publicar (externamente).
- ❏ Criar nova Política de Privacidade e publique (internamente).

2. Processos

- ❏ Mapeamento dos processos de trabalho que envolvam tratamento de dados pessoais e dados pessoais sensíveis, identificando o fluxo desses dados, a tecnologia utilizada, onde são armazenados e as pessoas envolvidas;
- ❏ Identificar quais dados pessoais são processados em qual processo de negócios;
- ❏ Motivar processos de dados pessoais ("propósito de processamento") para cada processo de negócios;
- ❏ Criar ou alterar o processo de avaliação de impacto da privacidade;
- ❏ Criar ou alterar o processo de avaliação de risco;
- ❏ Realizar avaliações de risco e privacidade para identificar lacunas iniciais ;
- ❏ Determinar e documentar fundamentos legais para processamento;
- ❏ Criar rotina para caso a autoridade nacional faça requisição de relatório. O controlador deverá inserir no, no mínimo, as seguintes informações:
- ❏ Descrição dos tipos de dados coletados;
- ❏ Metodologia utilizada para a coleta de dados;
- ❏ Metodologia utilizada para garantir a segurança das informações;
- ❏ Análise do controlador com relação a essas medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

Requisitos para aplicação da LGPD na saúde suplementar

3. Organização e Comunicação

- ❏ Nomear o Oficial de Proteção de Dados (DPO).
- ❏ Identificar as funções da própria organização e dos parceiros: Controladores de Dados / Processadores de dados.
- ❏ Estabelecimento de padrões mínimos para um Projeto de Governança da Informação e Proteção de Dados;
- ❏ Divulgação em veículos de fácil acesso a finalidade, práticas de execução e previsão de tratamento de dados públicos. Indicação de Encarregado da função para tal.
- ❏ Criar novo aviso de privacidade e publicar (externamente).
- ❏ Criar nova Política de Privacidade e publique (internamente).

4. Processos

- ❏ Mapeamento dos processos de trabalho que envolvam tratamento de dados pessoais e dados pessoais sensíveis, identificando o fluxo desses dados, a tecnologia utilizada, onde são armazenados e as pessoas envolvidas;
- ❏ Identificar quais dados pessoais são processados em qual processo de negócios;
- ❏ Motivar processos de dados pessoais ("propósito de processamento") para cada processo de negócios;
- ❏ Criar ou alterar o processo de avaliação de impacto da privacidade;
- ❏ Criar ou alterar o processo de avaliação de risco;
- ❏ Realizar avaliações de risco e privacidade para identificar lacunas iniciais ;
- ❏ Determinar e documentar fundamentos legais para processamento;
- ❏ Criar rotina para caso a autoridade nacional faça requisição de relatório. O controlador deverá inserir no, no mínimo, as seguintes informações:
- ❏ Descrição dos tipos de dados coletados;
- ❏ Metodologia utilizada para a coleta de dados;
- ❏ Metodologia utilizada para garantir a segurança das informações;
- ❏ Análise do controlador com relação a essas medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

Requisitos para aplicação da LGPD na saúde suplementar

5. Direitos do Titular

- ❏ Definição de mecanismos e garantias de Compliance com
- ❏ princípios e direitos do titular, conforme previsto em Lei;
- ❏ Desenvolver Plano de Contingência em caso de incidente envolvendo dados pessoais que possa implicar em risco ou danos relevantes aos titulares;
- ❏ Definir fluxo institucional e regramento interno para confirmação ou providências para o acesso e retificação de dados pessoais, mediante requisição do titular, em formato simplificado ou por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, fornecida no prazo de até 15 (quinze) dias;
- ❏ Criar portal de autoatendimento onde os sujeitos de dados podem executar ações para executar seus direitos.
- ❏ Garantir que os detalhes de contato do DPO estejam disponíveis para todos os assuntos de dados.

6. Proteção de Dados

- ❏ Rever o armazenamento atual de dados pessoais;
- ❏ Remover quaisquer dados pessoais que não atendam aos critérios de finalidade de processamento (incluindo Backups);
- ❏ Registrar as assinaturas dos proprietários do processo de negócios, indicando que seu processo é totalmente compatível;
- ❏ Realizar uma avaliação de risco se apropriado;
- ❏ Indicar Encarregado pelo tratamento dos dados pessoais, divulgando publicamente, de forma clara e objetiva,preferencialmente no seu sítio eletrônico, a identidade da pessoa e suas informações de contato. Em linhas gerais, as atividades do encarregado consistem em:
  - ❏ Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
  - ❏ Receber comunicações da autoridade nacional e adotar providências;
  - ❏ Orientar os funcionários e os contratados da organização a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

Requisitos para aplicação da LGPD na saúde suplementar

- ❏ Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares emitidas pela autoridade nacional de proteção de dados;
- ❏ Criar rotinas de registro das operações de tratamento de dados pessoais que realize, podendo a autoridade acional determinar que seja elaborado relatório de impacto à proteção de dados (pessoais ou sensíveis) referente às suas operações.

7. Gestão de conhecimentos

- ❏ Identificar todos os pontos de contato em que o consentimento dos dados é obtido;
- ❏ Identificar processos para os quais é necessário o consentimento;
- ❏ Identificar controladores de dados e processadores envolvidos com dados para os quais é necessário o consentimento;
- ❏ Revisar o gerenciamento de consentimento – se existente - no site e adaptar a LGPD;
- ❏ Revisar a gestão de consentimento existente em formulários em papel e adaptar a LGPD;
- ❏ Criar repositório para gerenciamento de consentimento para garantir que o ônus da prova possa ser facilitado.

8. Retenção de Dados e Backup

- ❏ Revisar os requisitos de retenção de dados existentes.
- ❏ Revisar os processos de backup existentes.
- ❏ Alterar as políticas de retenção de dados e os processos de backup.
- ❏ Remover todos os dados pessoais existentes em backups existentes.

9. Contratos

- ❏ Criar acordos controlador-processador onde ainda não estão em vigor;
- ❏ Atualizar os acordos do controlador-processador: uso intencional e requisitos de segurança;
- ❏ Atualizar outros acordos existentes, quando aplicável.
- ❏ Atualizar o processo de aquisição: critérios de seleção para novos serviços;
- ❏ Atualizar o processo de aquisição: novos requisitos incluídos emnovos contratos.

10. Plano de resposta a Violação de Dados

- ❏ O controlador responde solidariamente com o operador se, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à LGPD.

Leonardo Moreira
lmoliveira@mettricx.com
55 21 99407.3374