MANUAL LGPD – FUNEAS
SETOR HOSPITALAR

FUNEAS
Fundação Estatal de Atenção em Saúde do Paraná
PARANÁ
GOVERNO DO ESTADO
SECRETARIA DA SAÚDE

SUMÁRIO

1. PALAVRA DO PRESIDENTE..... 3
2. ALINHAMENTO COM A CULTURA DA ENTIDADE 3
3. A LGPD NO AMBIENTE HOSPITALAR 4
4. CONCEITOS LEGAIS DA LGPD..... 5
4.1. PRINCÍPIOS DA LGPD..... 5
4.2. DIREITO DOS TITULARES..... 6
4.3. OBRIGAÇÕES E RESPONSABILIDADES..... 7
5. COMO SE ADEQUAR À LGPD..... 7
5.1. PROGRAMA DE GOVERNANÇA EM PROTEÇÃO DE DADOS 7
5.2. AGENTES DE TRATAMENTO 8
5.3. AVALIAÇÃO E CONSCIENTIZAÇÃO 8
5.4. MAPEAMENTO 9
5.5 ANÁLISE DE GAPS, PLANEJAMENTO E IMPLEMENTAÇÃO.....9
5.6. PROTEÇÃO 9
5.7. MONITORAMENTO 10
6. BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS 10
7. CONCLUSÃO 11

1. PALAVRA DO PRESIDENTE

A aplicação das normas da Lei Geral de Proteção de Dados (LGPD) já é uma realidade, e o grande desafio que se apresenta para os hospitais públicos é a obtenção da segurança jurídica nas relações que mantém com pessoas físicas e jurídicas, necessária para a continuidade das suas atividades essenciais de saúde.

A adequação à nova LGPD é necessária e salvaguarda a segurança jurídica de todos os atores envolvidos no tratamento da informação: o hospital, o paciente e o profissional. A nova legislação está fundamentada em um conjunto de princípios e conceitos que a permite se adaptar ao dinamismo e à velocidade com que o mundo digital se transforma.

Na medida em que as atividades humanas passam a ser, cada vez mais, potencializadas pela mediação de tecnologias digitais, há uma exigência natural da sociedade para que essas relações levem em consideração a privacidade e a proteção dos dados pessoais em todos os âmbitos. A responsabilidade sobre o Setor Saúde se sobressai, sobretudo por ser aquele que mais trata de dados pessoais sensíveis – um dos focos primordiais da nova Lei.

A LGPD impõe boas práticas de governança e controle na gestão hospitalar para a proteção das informações que são coletadas, cotidianamente, no ambiente de trabalho.

Cabe lembrar que, mais que adaptação, a LGPD exige uma transformação da cultura organizacional em defesa do direito à privacidade, sob pena de pesadas sanções à FUNEAS.

2. ALINHAMENTO COM A CULTURA DA ENTIDADE

Antigamente, a questão da privacidade associava-se à busca por alguma forma de isolamento, refúgio ou segredo, o chamado “direito de estar só”. A partir da revolução tecnológica, porém, tal conceito tornou-se mais abrangente, passando a relacionar-se a outros escopos, como a procura por igualdade, liberdade de escolha, vontade de não ser discriminado e até mesmo ao desenvolvimento da personalidade. Em suma, pode-se afirmar que a proteção à privacidade é essencial para o ser humano: todos temos direito a não sermos incomodados, a termos nossas comunicações livres de interferência e ao sigilo das informações.

Nesse sentido, é correto afirmar que cada vez mais o fornecimento de dados realizado pelos próprios indivíduos, abre margem para diversas formas de tratamento, possibilitando a identificação dessas pessoas sem o seu devido conhecimento. Estas informações são estruturadas em grandes bancos de dados e consideradas como o principal fator em uma avaliação de crédito, na aprovação de um plano de saúde, na

obtenção de um emprego, na passagem pela migração em um país estrangeiro e em inúmeras outras situações.

O acúmulo de informações pode ser, também, uma grande fonte de renda para empresas privadas, que se utilizam do banco de dados para traçar hábitos de consumo, indicativos de personalidade e até mesmo informações íntimas de caráter privado de milhares de pessoas, vendendo-os para outras empresas com finalidades diversas, bem como a divulgação de produtos por e-mails ou por mensagens de texto.

Sob essa lógica, a Constituição Federal de 1988 estabelece, em seu Art. 5º, incisos X e XII (BRASIL, 1988), o direito à proteção à intimidade, assim como a inviolabilidade do sigilo de correspondências e das comunicações, protegendo, portanto, diversos aspectos que asseguram a privacidade dos cidadãos brasileiros. Contudo, ainda que exista tal previsão, é indiscutível que a vida em sociedade pressupõe o compartilhamento de informações, sendo, desse modo, necessária a compatibilização do direito à privacidade com a necessidade de circulação de dados. Tal processo se dá mediante a operação de atos regulatórios, que possibilitam aos cidadãos um efetivo controle de suas informações pessoais.

3. A LGPD NO AMBIENTE HOSPITALAR

A LGPD, responsável por melhor regulamentar o tratamento cedido a dados pessoais no território nacional, impactou de maneira significativa a atuação dos hospitais, em especial no que diz respeito à relação entre paciente e instituição.

Como sabido, as instituições hospitalares necessitam de informações e dados de pacientes para atuarem de maneira adequada. O tratamento destes dados, a partir da sanção da Lei, deve ocorrer em conformidade com alguns parâmetros específicos e, em se tratando dos dados relativos à saúde, receber tratamento peculiar, haja vista que os últimos são classificados como dados sensíveis pela LGPD.

Dados relativos à saúde, nos termos do Art. 4º da Lei (BRASIL, 2018), são aqueles relacionados com a saúde física ou mental de uma pessoa natural, incluindo a prestação de serviços, que revelem informações sobre o seu estado de saúde. Estes, assim como os demais dados sensíveis dispostos no texto legal, recebem uma proteção mais ampla, exigindo o consentimento explícito dos pacientes e uma finalidade específica – salvo em hipóteses excepcionais que os dispensem, como em casos de preservação da vida ou da integridade física.

A gestão do consentimento integra uma das bases legais mais importantes previstas pela LGPD. A organização hospitalar é encarregada de fornecer uma interface para que o indivíduo possa autorizar, bloquear ou revogar o consentimento para o tratamento de dados pessoais a qualquer momento. No mais, é obrigatório que haja, à disposição dos

pacientes, uma maneira fácil de revogar o seu consentimento e, ainda, que a instituição tenha um controle e um armazenamento de documentos relativos a ele (digitais ou físicos).

Retomando a noção de que os dados relativos à saúde devem ser obtidos em decorrência de uma finalidade específica, além de armazenar e cuidar dos dados dos pacientes, é dever da instituição informar ao público a razão que justifica a coleta de seus dados – o que, por conseguinte, evidencia a necessidade da devida conscientização de todos os funcionários do hospital para que sejam capazes de esclarecer eventuais dúvidas sobre a exigência de coleta daquelas informações.

A LGPD exige que as organizações tenham uma política clara e transparente para a coleta e o tratamento de dados, que deve ser amplamente divulgada para seus colaboradores e, também, para os titulares de seus dados. A conscientização – que, além dos funcionários, deve abranger os colaboradores e os parceiros – pode ser feita por meio de palestras, apresentações, videoconferências e até mesmo com pequenos informes enviados aos funcionários de tempos em tempos.

O compartilhamento de dados pode, muitas vezes, apresentar grande risco, pois as pessoas, mediante a exposição de elementos sensíveis sobre si mesmas ou sobre familiares, possibilitam que tais informações sejam utilizadas para práticas ilícitas, como fraudes e crimes – no mundo digital ou não. A cultura de proteção de dados, nesse contexto, há de ser urgentemente difundida, a fim de proteger a grande maioria da população que, alheia aos riscos inerentes ao compartilhamento, expõe-se demasiadamente (seja em suas redes sociais, seja realizando cadastros para receber descontos ou brindes).

4. CONCEITOS LEGAIS DA LGPD

4.1. PRINCÍPIOS DA LGPD

A LGPD possui dez princípios, além da boa-fé, que devem ser observados por todos aqueles que tratarem dados pessoais. São eles:

(i) Finalidade: simboliza que as finalidades para o tratamento dos dados pessoais devem ser legítimas, específicas, explícitas e informadas ao titular;

(ii) Adequação: significa que as atividades devem ser condizentes com a destinação para a qual os dados pessoais foram coletados;

(iii) Necessidade: implica a coleta da menor quantidade possível de dados pessoais para cada atividade;

(iv) Livre acesso: possibilita que os titulares tenham acesso de forma fácil à consulta sobre os seus dados pessoais que estejam sendo tratados;

(v) Qualidade dos dados pessoais: assegura aos titulares o direito de que os dados pessoais estejam corretos e atualizados;

(vi) Transparência: garante aos titulares que as informações sobre as atividades de tratamento de dados pessoais estejam em linguagem clara e simples;

(vii) Segurança: obriga os agentes de tratamento de dados pessoais a se utilizarem de medidas técnicas e administrativas aptas a proteger estes dados;

(viii) Prevenção: obriga os agentes de tratamento de dados pessoais a adotarem medidas para prevenir a ocorrência de danos em virtude do tratamento;

(ix) Não discriminação: impossibilita o tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos;

(x) Responsabilização e prestação de contas: os agentes de tratamento de dados pessoais devem adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção aos dados pessoais, atestando, inclusive, a eficácia dessas medidas.

4.2. DIREITO DOS TITULARES

Inicialmente, a LGPD informa que toda pessoa natural tem assegurados e garantidos os seus direitos fundamentais de liberdade, intimidade e privacidade, o que é essencial, pois, como vimos no início desta cartilha, a proteção de dados visa complementá-los.

Outros direitos garantidos ao titular de dados pessoais são:

(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 a Lei;

(v) Portabilidade dos dados pessoais (ou seja, a transferência dos dados pessoais de um controlador a outro, desde que assegurados os segredos industrial e comercial);

(vi) Eliminação dos dados pessoais tratados sob a base legal do consentimento;

(vii) Informações sobre o compartilhamento de dados pessoais;

(viii) Informações sobre a possibilidade de não fornecer o consentimento e sobre as consequências de tal conduta;

(ix) Revogação do consentimento.

4.3. OBRIGAÇÕES E RESPONSABILIDADES

A LGPD, além de diferenciar os agentes de tratamento, dispõe sobre as obrigações e as responsabilidades no caso de danos decorrentes do tratamento inadequado de dados pessoais e de incidentes relativos à segurança da informação.

A principal obrigação dos agentes acima citados é, de acordo com a Lei, que mantenham um registro das operações de tratamento que realizarem, especialmente quando este tratamento de dados pessoais ocorrer segundo a base legal do legítimo interesse.

No que diz respeito especificamente à atuação do operador, este deverá realizar o tratamento de dados pessoais conforme as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. É necessário que todas as instruções sejam claras e, preferencialmente, formais, para que não haja incerteza ou falha no processo de tratamento de dados pessoais.

5. COMO SE ADEQUAR À LGPD

5.1. PROGRAMA DE GOVERNANÇA EM PROTEÇÃO DE DADOS

Para garantir o efetivo cumprimento das normas, o Art. 50 da LGPD estipula um capítulo exigindo que:

"sejam formuladas regras sobre boas práticas e governança, que estabeleçam as condições, 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 agentes envolvidos no tratamento dos dados pessoais, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais."

Cada política, norma e ação criada dentro da instituição deve ser documentada, de modo a demonstrar a efetividade de seu programa de governança quando houver

questionamento e, em especial, a pedido da ANPD. A adoção de tais políticas não apenas auxilia o cumprimento das obrigações estabelecidas pela Lei, como demonstra os esforços nesse sentido, e todos os registros documentados das ações adotadas serão considerados em uma eventual aplicação de sanção por tratamento inadequado de dados pessoais.

Além disso, mesmo que já exista um conjunto de políticas do hospital, é importante garantir que elas estejam de acordo com a nova Lei: devem estar incluídas no seu conjunto de políticas todas aquelas referentes à segurança da informação, à privacidade, à classificação da informação e ao controle de acesso.

5.2. AGENTES DE TRATAMENTO

A LGPD estabelece como agentes de tratamento os indivíduos encarregados de controlar ou tratar as informações que contenham dados pessoais. São eles:

a) Controlador: a pessoa física ou jurídica que determina como todo e qualquer tratamento de dados pessoais ocorrerá;

b) Operador: a pessoa física ou jurídica que segue as determinações vindas do controlador para elaborar o tratamento de dados pessoais.

Em suma, a diferença entre o controlador e o operador reside no escopo da função: o primeiro é responsável pela coleta dos dados pessoais dos titulares, enquanto ao segundo cabe a realização do tratamento destes dados em virtude de contrato, respeitando as instruções do controlador.

Embora a Lei não o defina como agente de tratamento, vale destacar a figura do encarregado, pessoa indicada pelos agentes de tratamento para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

5.3. AVALIAÇÃO E CONSCIENTIZAÇÃO

Como previamente mencionado, a eficácia do programa de adequação à LGPD exige a devida conscientização de todos os profissionais que trabalham dentro do hospital, bem como de eventuais colaboradores. A cultura de proteção de dados deve, impreterivelmente, ser amplamente difundida, haja vista que o programa somente existe com a participação de todos.

Deve-se, nesse contexto, levar em consideração o quanto de informação sobre o projeto os funcionários possuem e, a partir desse ponto, conscientizá-los acerca do objetivo do projeto, bem como sua estruturação. A instituição deve se familiarizar com a LGPD, com a metodologia do projeto, e entender que todas as atividades serão averiguadas.

5.4. MAPEAMENTO

A LGPD determina que o controlador e o operador mantenham registro das operações de tratamento de dados pessoais que realizarem, desde a etapa de mapeamento de processos, momento de grande importância para a adequação da empresa.

Nesta ocasião, será possível:
(i) detalhar cada dado pessoal tratado, entendendo as fases do seu ciclo de vida;
(ii) perceber como estes dados são recebidos, de que forma e onde estão armazenados, quem tem acesso e se são compartilhados com terceiros; e, ainda,
(iii) analisar seus riscos associados a cada operação, bem como a base legal adequada.

Em suma, é fundamental que todo processo hospitalar que envolva uso de dados pessoais seja mapeado. Essa atividade não só colabora com a identificação dos riscos, como auxilia na minimização da coleta, garantindo que as informações obtidas sejam somente aquelas necessárias para cumprir com sua finalidade.

5.5. ANÁLISE DE GAPS, PLANEJAMENTO E IMPLEMENTAÇÃO

Após o mapeamento dos processos, será possível identificar diversas questões em desacordo com a LGPD ou com as melhores práticas de segurança da informação, ou, ainda, com as práticas setoriais aplicáveis. Neste momento, deve-se definir as bases legais adequadas para cada atividade de tratamento de dados pessoais executadas na instituição, bem como elaborar um relatório com os principais gaps, apontando quais são as medidas necessárias para a mitigação de riscos envolvendo incidentes de segurança da informação.

Analisados os gaps, será necessário verificar quais são as prioridades da empresa, assim como elaborar um cronograma para mitigar os riscos localizados nas etapas anteriores. No mais, deve haver a indicação de responsáveis para cada atividade de tratamento com necessidade de alteração e a verificação dos diferentes níveis de criticidade de cada medida.

Por último, é chegada a hora de adequar as medidas em desconformidade com a legislação. Neste momento, é imprescindível adequar plataformas, processos, contratos, práticas e documentos que versem sobre o tratamento de dados pessoa

5.6. PROTEÇÃO

Recomenda-se que a instituição invista em equipamentos com bases de proteção atualizadas constantemente, com especial importância em um ambiente crítico como o hospital. Novas formas de ataque surgem periodicamente, e é preciso criar proteção

contra elas dentro dos sistemas, além de garantir a disponibilidade de manutenção até mesmo em horários não comerciais ou aos fins de semana.

5.7. MONITORAMENTO

Depois de finalizada a etapa de implementação, encerra-se o projeto de adequação à LGPD. Entretanto, é impossível afirmar que projetos desse tipo, de fato, chegam a um fim definitivo, pois a organização deve, de modo constante, avaliar se está de acordo com a legislação de proteção de dados pessoais. A própria legislação é mutável no que tange à alteração e à regulamentação, o que mostra que a empresa precisará se adequar às novidades no cenário da privacidade.

Dessa maneira, é essencial que a instituição tenha funcionários (internos, externos ou mesmo uma equipe híbrida) capazes de monitorar todas as novidades ocorridas, garantindo, assim, que a organização nunca esteja desatualizada ou sofra alguma sanção eventualmente imposta pela ANPD.

Outro ponto fundamental do monitoramento é a necessidade de treinamentos com certa periodicidade, para que a cultura da proteção aos dados pessoais seja parte do dia a dia do hospital.

6. BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS

Para que uma atividade de tratamento de dados pessoais seja realizada, é necessário saber sob qual fundamento de legalidade esta atividade está baseada. A LGPD afirma que, para todo tratamento de dados pessoais, deve haver uma norma legal que o fundamente. A seguir estão as bases legais expostas na Lei:

(i) Para o cumprimento de uma obrigação legal ou regulatória: quando a empresa for obrigada a realizar uma atividade de tratamento de dados pessoais objeto de lei ou regulamentação;

(ii) Realização de estudos por órgão de pesquisa: somente órgãos de pesquisa poderão usar essa base legal para tratar dados pessoais. O tratamento deve ser utilizado para fins de pesquisa e estudos, devendo, sempre que possível, anonimizar dados pessoais;

(iii) Execução de contratos em que o titular seja parte: quando o titular de dados pessoais celebrar um contrato ou mesmo em procedimentos preliminares à celebração de um contrato;

(iv) Exercício regular de direitos em processo judicial, administrativo ou arbitral: quando a empresa ajuizar uma ação em face de um cidadão, seus dados pessoais poderão ser tratados sem que isso represente uma violação;

(v) Proteção da vida ou da incolumidade física do titular ou de terceiro: esta é uma base legal muito importante, pois permite o tratamento de dados pessoais quando um titular estiver em risco de vida. Por exemplo: quando um cidadão é levado a um hospital após sofrer um grave acidente;

(vi) Para a tutela da saúde, em procedimento realizado por profissionais da saúde: utilizada quando, por exemplo, um cidadão se dirige a uma farmácia pública para obter remédios. O farmacêutico deverá ter acesso aos dados pessoais deste cidadão para verificar a medicação e realizar os controles necessários;

(vii) Para atender aos interesses legítimos do controlador ou de terceiro: pode ser utilizada para fundamentar atividades de tratamento de dados pessoais que tenham finalidades legítimas, consideradas a partir de situações concretas, como apoio e promoção de atividades da empresa, bem como para proteger os titulares de dados do exercício regular de seus direitos ou prestação de serviços que o beneficiem;

(viii) Para a proteção do crédito: esta base legal pode ser utilizada para serviços de proteção ao crédito.

Ressalta-se que, no caso de tratamento de dados pessoais sensíveis, não poderá ser utilizada a base legal do interesse legítimo. Além disso, segundo a LGPD, para o tratamento dos dados pessoais sensíveis o titular precisará ser informado exatamente para quais finalidades os seus dados pessoais serão tratados, devendo expressar o seu consentimento em uma cláusula em separado e em destaque do contrato original (por exemplo: assinando um anexo).

Há outra base legal para o tratamento de dados pessoais sensíveis, para a garantia de prevenção à fraude e da segurança do titular, em processos de identificação e autenticação de cadastro em sistemas eletrônicos: quando, por exemplo, é utilizada a biometria para acessar uma conta em um caixa eletrônico.

7. CONCLUSÃO

O objetivo final deste manual é orientar sobre os conceitos básicos afetos à LGPD, visando informar e engajar quanto à adequação da FUNEAS à Lei.

Todas as unidades da FUNEAS serão envolvidas no processo de adequação à LGPD, uma vez que o objetivo final é fortalecer a cultura de segurança de dados pessoais e dados pessoais sensíveis tratados no âmbito da Fundação.