cbr | Colégio Brasileiro de Radiologia e Diagnóstico por Imagem

LGPD

LEI GERAL DE PROTEÇÃO DE DADOS

Valério Ribeiro
OAB/MG 74.204

Davi Coelho
OAB/MG 215.033

Fábio Visentin
OAB/MG 190.650

Lei Geral de Proteção de Dados – LGPD

I – Introdução:

Em setembro de 2020, entrou em vigor a Lei Geral de Proteção de Dados – LGPD, Lei 13.709/18, a qual dispõe sobre o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, sendo aplicável em todo o território nacional e vinculando União, Estados e Municípios.

O referido diploma legal tem como escopo a proteção dos dados pessoais, respeitando a privacidade, a autodeterminação informativa, a liberdade de expressão, a inviolabilidade da intimidade, entre outros direitos. Apesar de ser uma legislação recente nesse sentido, não é a primeira a abordar tais questões.

Em 1988, ao ser promulgada, a Constituição Federal já previa a inviolabilidade da intimidade, vida privada, honra e imagem, assegurando indenização por violações a esses atributos da personalidade, conforme descrevem os artigos 5º, V e X[1] da Carta Política.

Complementando as diretrizes constitucionais, o Código Civil de 2002 também destaca, nos artigos 12 e 21[2], que a prática dos direitos individuais não está sujeita a restrições voluntárias, e o detentor desses direitos pode solicitar ao juiz a tomada de medidas adequadas para evitar ou interromper qualquer ação contrária a essa norma.

[1] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
...
V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;
...
X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

[2] Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei.
...
Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

Na mesma esteira, o Código de Defesa do Consumidor[3], Lei 8.078/90, que é norteado pelos conceitos de informação adequada e prevenção, congrega disposições protetivas da dignidade, saúde e segurança dos consumidores, compondo também o arcabouço legal de blindagem aos diretos da personalidade.

A Lei Geral de Proteção de Dados – LGPD[4], Lei 13709/2018, por sua vez, propõe-se a fornecer transparência e segurança no tratamento de dados pessoais, não apenas no mercado de consumo, mas em qualquer relação em que haja o tratamento de informações pessoais.

No que diz respeito à territorialidade, a Lei Geral de Proteção de Dados é aplicável sempre que ocorrer o processamento e/ou a coleta de dados em solo nacional ou quando houver a oferta de bens e serviços, mesmo que estrangeiros, para pessoas localizadas no Brasil.

Portanto, é essencial que todas as entidades que tratam dados no território brasileiro se adaptem à LGPD para evitar penalidades significativas por infrações à legislação.

II – Adequação à LGPD para Hospitais e Clínicas. Passos Iniciais:

Vivencia-se hoje um avanço tecnológico sem precedentes. A cada dia que passa é possível testemunhar a criação de novos aparelhos eletroeletrônicos, novos aplicativos, novos sistemas e interagir mais intensamente com essas novas

[3] Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios:
I - reconhecimento da vulnerabilidade do consumidor no mercado de consumo;

[4] Art. 1º Esta Lei 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.
Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

tecnologias. Não há como viver ou sobreviver alijado das conexões digitais, da internet das coisas e da inteligência artificial, apenas para citar três exemplos.

Se de um lado as maravilhas tecnológicas trazem um mundo novo de conforto e praticidade para os seus usuários, de outro traz o risco da exposição dos dados destes usuários a terceiros que podem utilizar tais informações pessoais para finalidades que não condizem com o interesse legítimo de seus titulares.

É neste contexto que tem importância o debate acerca das medidas necessárias e indispensáveis para a proteção da privacidade, intimidade e da autodeterminação do particular na gestão de seus dados, no contexto das informações digitais.

Atento a esse cenário e tendo em vista a vigência da Lei nº 13709/2018 (LGPD), o Colégio Brasileiro de Radiologia e Diagnóstico por Imagem edita um breve um breve resumo acerca das medidas necessárias para adequação de Hospitais e Clínicas à Lei Geral de Proteção de Dados.

III – Dados Sensíveis e Necessidade de Implementação de uma Política de Proteção de Dados por Hospitais e Clínicas:

Conforme explicitado na introdução acima, a LGPD visa trazer uma proteção aos dados pessoais de particulares tendo em vista que, hoje em dia, tais dados possuem um elevado valor econômico, de modo que empresas e agentes escusos podem se usurpar de informações pessoais para, por exemplo, direcionar conteúdos, controlar padrões de compras, vazar informações, enfim, promover uma ingerência indevida na esfera de privacidade dos titulares dos.

Neste contexto, a Lei nº 13.709/2018, dá especial relevância aos chamados dados pessoais sensíveis, definindo-os como "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"[5].

Fica evidente, portanto, que os dados referentes à saúde de uma pessoa são considerados dados pessoais sensíveis e, por isso mesmo, detém uma especial proteção da legislação, tendo em vista que dizem respeito, em última instância, à própria personalidade do seu titular.

[5] Artigo 5º, II da Lei 13.709/2018.

Sendo assim, é de suma importância que os Hospitais e Clínicas que prestam serviços de saúde, pública ou particular, se adequem à uma política de proteção de dados, para evitar, por exemplo, que prontuários e receituários médicos de seus pacientes sejam utilizados para finalidades distintas e estranhas à prestação de serviços na área da saúde.

Tendo isto em mente, nos próximos tópicos será exposto um ponto de partida para a implementação de uma política de proteção de dados no âmbito de empresas atuantes na área da saúde.

IV – Saiba Quais Dados seu Hospital ou Clínica Coletam:

Assim como na área médica é imprescindível realizar um diagnóstico para saber qual a enfermidade do paciente e quais os procedimentos e técnicas mais adequados para o seu tratamento. Uma boa política de dados passa pelo "diagnóstico" à respeito da quantidade e qualidade das informações pessoais que estão sendo coletados pela empresa atuante na área da saúde.

Sendo assim, o primeiro passo dos serviços médicos para adequação à LGPD é reunir todas as informações que possuí a respeito dos seus pacientes, sendo tal passo essencial para que se possa compreender a real situação em relação à proteção de dados dos seus clientes.

Neste sentido é importante observar:

1. Quais são os tipos de dados coletados pelo serviço na área da saúde?
2. Como é feito o tratamento de dados pela clínica ou hospital?
3. Com qual finalidade tais dados são coletados?
4. O que é feito com os dados após o término da prestação de serviços?
5. Como é feita a segurança dos dados coletados pela clínica ou hospital? e,
6. Como é feito o compartilhamento destes dados com terceiros, se isto ocorrer na empresa?

Portanto, é importante diagnosticar não só a qualidade e a quantidade de dados tratados, como, também, a forma de tratamento, ou seja, de colheita, manejo e exclusão de tais dados pela empresa prestadora de serviços em saúde.

V – Verificar se o Tratamento de Dados Feito pela Empresa está Adequado à LGPD:

Sabendo quais dados a empresa coleta, o segundo passo é organizá-los, identificando a natureza de cada informação utilizada, ou seja, se são dados pessoais (art. 5º, I, LGPD)[6], dados pessoais sensíveis (art. 5º, II, LGPD)[7], dados anonimizados (art. 5º, III, LGPD)[8] ou dados de crianças e adolescentes (art. 14, LGPD)[9].

Com a referida organização há que se verificar se o tratamento dessas informações pessoais, ou seja, se a coleta, produção, reprodução, transmissão, avaliação, modificação, arquivamento e exclusão de dados, estão sendo realizados em conformidade com a LGPD.

Para tanto deverá ser:

1. Observado se há o consentimento livre e esclarecido do particular para o tratamento dos dados contendo, inclusive, a finalidade para a qual tais dados serão tratados;
2. Avaliado se o ciclo de tratamento de dados é seguro para o cliente;
3. Verificado se o compartilhamento de dados está sendo realizado de forma segura e clara; e,
4. verificar se é garantida a comunicação do titular de dados com a empresa que realiza o seu tratamento.

As atitudes expostas acima norteiam-se, principalmente, pelo princípio da autodeterminação informativa (art. 2º, II, LGPD)[10], segundo o qual o particular tem

[6] Artigo 5º Para os fins desta Lei, considera-se:
I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
[7] II - dado pessoal sensível: 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;
[8] III - 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;
[9] Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
[10] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

o direito de gerir todos os seus dados devendo, por isso, dar o seu consentimento livre, esclarecido e "desviciado" à respeito dos seus dados que estão sendo coletados e tratados, bem como acerca da finalidade do tratamento de seus dados.

É importante esclarecer que o titular dos dados é sempre o particular, de modo que ele tem total liberdade para definir o que será feito com suas informações pessoais. Sendo assim, é imprescindível que ele esteja ciente de todo tipo de tratamento ou compartilhamento de seus dados.

Portanto, em se tratando de empresas que prestam serviços de saúde, é interessante colher, sempre que possível, o consentimento por escrito do paciente, para eventual envio de prontuário médico para outro profissional ou para diferentes setores dentro de um hospital ou clínica, por exemplo.

VI – Verificar se os Princípios da LGPD e se os Direitos dos Usuários estão Sendo Respeitados:

Os princípios norteadores da Lei Geral de Proteção de Dados podem ser encontrados no seu art. 6º, sendo esta uma norma de cunho explicativo, ou seja, que não só indica, como também, traz uma explicação acerca de cada princípio apresentado. Nestes termos, por motivos de conveniência, colaciona-se o mencionado artigo.

> "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

> III - 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;
> IV - 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;
> V - 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;
> VI - 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;
> VII - 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;
> VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - 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.” (destacamos)

Para a adequação à LGPD todo o tratamento de dados feito pela clínica ou hospital deverá ser norteado por todos os princípios acima indicados.

No que diz respeito aos direitos dos usuários, a LGPD reserva o seu Capítulo III especificamente para o tema, disciplinando a matéria nos artigos 17 a 22.

Para não fugir ao objetivo desse breve resumo, são direitos do particular:

1. A confirmação da existência de tratamento de dados;
2. O acesso aos seus dados;
3. A correção de dados incompletos, inexatos ou desatualizados;
4. A anonimização[11], bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD;
5. A portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, observados os segredos comercial e industrial;
6. A eliminação dos dados pessoais tratados com o consentimento do titular;
7. Informação das entidades públicas e privadas com as quais o controlador realizou o uso compartilhado de dados;
8. Informação sobre a possibilidade de não fornecer o consentimento e sobre as consequências dessa negativa; e,
9. A impossibilidade do consentimento, como é de se perceber do rol do art. 18 da LGPD.

VII – Do Compartilhamento de Dados:

Sabe-se, ainda, que na área médica é comum a necessidade de compartilhamento de documentos que contém dados pessoais sensíveis, tais como laudos, prontuários e receituários de pacientes.

Não raras vezes o atendimento assistencial é prestado por uma equipe multidisciplinar de profissionais na área da saúde, que compartilham entre si as informações, sintomas, exames, prognósticos, etc, dos pacientes por eles assistidos.

Sendo assim, é importante que a empresa se resguarde, adotando todas as ressalvas feitas pela LGPD no que diz respeito ao compartilhamento de dados.

[11] A anonimização é uma técnica de processamento de dados que remove ou modifica informações que possam identificar uma pessoa. Essa técnica resulta em dados anonimizados, que não podem ser associados a nenhum indivíduo específico.

De acordo com o artigo 5º, XVI, da LGPD, uso compartilhado de dados pode ser definido como "comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.".

Nestes termos, para o compartilhamento de dados ser realizado, de acordo com as normas da LGPD, em primeiro lugar deverá ser sempre observada a autodeterminação informativa do particular, que deverá dar seu consentimento livre e esclarecido com finalidade específica para a troca de informações, conforme dispõe o artigo 7º, §5º[12], da LGPD.

Além disso, o usuário deverá ter acesso a todas as informações referentes ao uso compartilhado de seus dados, bem como ter plena ciência da finalidade deste compartilhamento, consoante descreve o artigo 9º, V[13], da LGPD.

Finalmente, tratando especificamente da área da saúde, é importante pontuar que o artigo 11, §4º, da LGPD determina que é vedada a comunicação ou o uso compartilhado de dados pessoais sensíveis referentes à saúde com o objetivo de obter vantagem econômica, salvo algumas exceções, as quais, por sua importância, serão colacionadas abaixo:

> "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: (...)
> ...
> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde

[12] § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

[13] Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
...
V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

> que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:
> I - a portabilidade de dados quando solicitada pelo titular;
> II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.
> § 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários."

VIII – Da Política de Privacidade e Política de Cookies:

Para o tratamento de dados pelo serviço ou mesmo por um site/aplicativo, é necessário que se crie uma Política de Privacidade, bem como uma Política de Cookies com o objetivo de estabelecer regras e informar para os particulares, de modo transparente, como é feito o tratamento de dados pela empresa.

A partir da implementação desta política o usuário terá plena ciência à respeito de seus direitos, bem como da colheita de seus dados pessoais. Enfim, o titular da informação poderá compreender melhor todo o processo de tratamento de seus dados pessoais.

Nestes termos, de forma resumida, política de privacidade pode ser definida como o documento que traz todas as informações à respeito do tratamento de dados por uma empresa e dos direitos dos seus clientes, estando nele incluídos as medidas de segurança adotadas pela empresa com relação aos dados coletados de seus clientes.

Os Cookies, por sua vez, já podem ser considerados como parte do cotidiano. Quantas vezes, ao navegar pelos mais diversos sites, é possível observar uma janela aberta informando que o site trabalha com a colheita de cookies? Definindo em termos simples, os Cookies se destinam a capturar dados dos particulares que navegam por um site ou aplicativo, sendo de extrema importância para determinar como o usuário se comporta na rede e, através de algoritmos, personalizar o conteúdo que é destinado àquele usuário.

Sendo assim, uma política de Cookies é utilizada para informar ao usuário, em primeiro lugar, a captura de dados mediante este mecanismo e, em segundo lugar, informar a este usuário como os dados capturados desta maneira são tratados.

IX – Das Consequências da não Observância à LGPD:

Finalmente, cabe informar que a não observância aos preceitos contidos na LGPD, ou seja, a falta de compromisso com a proteção de dados pessoais poderá levar à sérias consequências seja na esfera cível, onde o particular poderá acionar a empresa em eventual Ação de indenização por danos materiais ou morais, ou na esfera administrativa, com a imposição de multas pesadas em desfavor do infrator.

No que diz respeito à esfera administrativa, a partir de 01/08/2021 entraram em vigor as sanções administrativas previstas na Lei nº 13.709/2018 (LGPD), as quais estão dispostas no artigo 52[14] da lei em comento

Portanto, como medida de prevenção, é imprescindível que os serviços médicos atuantes na área da saúde se adequem à LGPD.

X – Do Encarregado (Data Protection Officer – DPO) e suas Funções:

[14] 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: (Vigência)
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 - 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.

A Lei 13.709/18 (LGPD) determina, em seu artigo 5º, VIII[15], que o Encarregado, conhecido também pela sigla DPO (Data Protection Officer), nomenclatura trazida na GDPR (lei europeia), é a pessoa designada pelo controlador e operador para servir como ponto de contato entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Nos termos do artigo 41[16] da LGPD, o controlador deve nomear um Encarregado para lidar com os dados pessoais.

Neste sentido, tendo em vista que o Encarregado funcionará como canal de comunicação entre o controlador, os titulares dos dados e a ANPD, é fundamental que sua identidade e informações de contato sejam divulgadas de maneira pública, clara e direta, de preferência por meio do site do controlador.

O Encarregado poderá ser uma pessoa física ou jurídica. Destaca-se que não é obrigatório ser um profissional do direito, mas é necessário que o profissional nomeado DPO tenha conhecimento legal e técnico que permitam a realização da função.

Logo, mesmo sem formação jurídica, é essencial que o responsável esteja familiarizado com a lei.

Ressalta-se, ainda, que o responsável não desempenha o papel de operador de dados, mas, sim, um papel crucial como elo de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), exercendo as seguintes funções:

1. Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
2. Receber comunicações da autoridade nacional e adotar providências;
3. Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

[15] VIII - 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);
[16] Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

4. Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Outro ponto relevante sobre o DPO é sobre a obrigatoriedade de existência dessa função. A empresa poderá ser dispensada da nomeação de um DPO caso não possua uma quantidade significativa de dados a serem manuseados.

Nesse contexto, é válido citar a Resolução nº 2 CD/ANPD, divulgada em 27 de janeiro de 2022, a qual define, em seu artigo 2º, I, que agentes de tratamento de pequeno porte são microempresas, empresas de pequeno porte, startups, pessoas jurídicas de direito privado, inclusive sem fins lucrativos, nos termos da legislação vigente, bem como pessoas naturais e entes privados despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador.

Referida Resolução esclarece, ainda, em seu artigo 11, que:

> Art. 11. Os agentes de tratamento de pequeno porte não são obrigados a indicar o encarregado pelo tratamento de dados pessoais exigido no art. 41 da LGPD.
> § 1º O agente de tratamento de pequeno porte que não indicar um encarregado deve disponibilizar um canal de comunicação com o titular de dados para atender o disposto no art. 41, § 2º, I da LGPD.
> § 2º A indicação de encarregado por parte dos agentes de tratamento de pequeno porte será considerada política de boas práticas e governança para fins do disposto no art. 52, §1º, IX da LGPD.

Embora não seja obrigatório nomear um Encarregado, o agente de tratamento de pequeno porte, para se adequar às disposições da LGPD, precisa fornecer um meio de comunicação com o titular de dados para atender às exigências legais. Isso implica servir como uma ponte de comunicação com os titulares de dados, oferecendo esclarecimentos conforme necessário e tomando as medidas apropriadas conforme exigido.

A Resolução nº 2 CD/ANPD também observa que, mesmo que os agentes de tratamento de pequeno porte não sejam obrigados a nomear um Encarregado, fazê-

lo será considerado uma prática de boas políticas e governança e mitigadora de sanções, conforme estipulado no artigo 52, §1º, inciso IX da LGPD.

É relevante salientar que esse reconhecimento é significativo, pois em caso de violação da lei, essa medida pode ser considerada para atenuar as sanções aplicadas contra o agente de tratamento.

Além disso, em relação ao Encarregado, é importante esclarecer que, de acordo com a LGPD, ele não tem responsabilidade civil perante os titulares de dados e a ANPD, uma vez que as decisões sobre o tratamento de dados são de responsabilidade do controlador.

No entanto, é válido ressaltar que o Encarregado pode ser responsabilizado perante os agentes de tratamento, uma vez que é contratado para desempenhar funções relacionadas à comunicação entre os titulares, os controladores e a ANPD.

É importante destacar que o Encarregado poderá ser uma pessoa terceirizada no âmbito do tratamento de dados.

Assim, observa-se que o Encarregado ou DPO desempenha um papel crucial no cumprimento da LGPD.

XI – Proteção de Dados e Diretrizes do Conselho Federal de Medicina:

Conforme já esclarecido anteriormente, a Lei Geral de Proteção de Dados Pessoais – LGPD, Lei nº 13.709/2018, veio apenas robustecer o conceito de proteção a dados pessoais presente em nosso ordenamento jurídico. A preocupação com a proteção das informações pessoais é algo que existe desde a promulgação da Constituição Federal.

Neste diapasão, em 11 de julho de 2007, o Conselho Federal de Medicina, diante da evolução tecnológica e do crescente número de dados a serem armazenados pelos estabelecimentos de saúde, aprovou a Resolução nº 1.821/2007, a qual aprovou as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde.

Referida Resolução, em seu artigo 1º[17], demonstrou que já havia, naquele tempo, a preocupação do CFM com a segurança dos dados do paciente, haja vista que o próprio Conselho, junto com a Sociedade Brasileira de Informática em Saúde (SBIS), desenvolveu o Manual de Certificação para Sistemas de Registro Eletrônico em Saúde.

O referido manual foi criado com o objetivo de eliminar o papel utilizado para armazenamento dos dados do pacientes. Para isso, o documento citado criou níveis de segurança, quais sejam, Nível de Segurança 1 (NGS1) e Nível de Segurança 2 (NGS2).

O NGS1, possui um bom nível de segurança, entretanto, a eliminação do papel só é possível com a utilização de certificado digital padrão ICP-Brasil, segundo determinação da legislação em vigor sobre documento eletrônico no Brasil.

Já o NGS2 possui um nível ainda maior de segurança, garantindo a eliminação do papel, vez que especifica a utilização de certificados digitais ICP-Brasil para os processos de assinatura e autenticação.

Dessa forma, os sistemas de segurança estabelecidos no Manual de Certificação para Sistemas de Registro Eletrônico em Saúde se tornaram referência para questões médicas mais avançadas, inclusive, a Telerradiologia.

A Resolução nº 2.107/2014[18], por sua vez, a qual define e normatiza a Telerradiologia, com o objetivo de garantir a segurança e privacidade de dados dos pacientes, afirma que:

> Os sistemas informatizados utilizados para transmissão e manuseio dos dados clínicos, dos laudos radiológicos, bem como para compartilhamento de imagens e informações, devem obedecer às normativas do Conselho Federal de Medicina. Especificamente para telerradiologia, os sistemas devem atender aos requisitos obrigatórios do "Nível de Garantia de Segurança 2 (NGS2)", estabelecida no Manual de Certificação para Sistemas de Registro

[17] Art. 1º Aprovar o Manual de Certificação para Sistemas de Registro Eletrônico em Saúde, versão 3.0 e/ou outra versão aprovada pelo Conselho Federal de Medicina, anexo e também disponível nos sites do Conselho Federal de Medicina e Sociedade Brasileira de Informática em Saúde (SBIS), respectivamente, www.portalmedico.org.br e www.sbis.org.br.

[18] https://sistemas.cfm.org.br/normas/arquivos/resolucoes/BR/2014/2107_2014.pdf

Eletrônico em Saúde vigente, editado pelo CFM e Sociedade Brasileira de Informática em Saúde (SBIS).

Portanto, além das adequações gerais relacionadas a LGPD, as clínicas de Radiologia que utilizam a Telerradiologia e/ou fazem a transmissão de exames devem se adequar, também, às especificidades da Resolução nº 2.107/2014 e do Manual de Certificação para Sistemas de Registro Eletrônico em Saúde vigente.

XII – Conclusão:

Como informado no tópico inicial, o presente documento tem como objetivo apresentar um resumo, em linhas gerais, para a adequação de hospitais e clínicas às normas trazidas pela Lei Geral de Proteção de Dados.

Contudo, em se tratando de matéria intrinsecamente ligada à tecnologia, cabe a ressalva de que a adequação total de empresas à LGPD poderá depender da prestação de serviços de profissionais especializados na área de Tecnologias da Informação, na medida em que a mera adequação à formalidade da Lei não garante a proteção, de fato, aos dados coletados pelo serviço médico.

A despeito disso, esperamos que este breve documento, produzido pelo Colégio Brasileiro de Radiologia e Diagnóstico por Imagem, tenha o condão de informar seus parceiros e associados acerca das medidas iniciais para se proceder com a adequação de hospitais e clínicas às exigências trazidas pela LGPD e pelo próprio CFM.

Colégio Brasileiro de Radiologia
e Diagnóstico por Imagem