SBOT
SOCIEDADE BRASILEIRA DE ORTOPEDIA E TRAUMATOLOGIA

LGPD

LEI GERAL DE PROTEÇÃO DE DADOS

Valério Ribeiro
OAB/SP 451.277

Davi Coelho
OAB/MG 215.033

Manual Lei Geral de Proteção de Dados

Introdução

Em setembro de 2020, entrou em vigor a Lei Geral de Proteção de Dados (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.

Complementando as diretrizes constitucionais, o Código Civil de 2002 também destaca, nos artigos 11 e 21, que a prática dos direitos individuais não está sujeita a restrições voluntárias, e o detentor desses direitos pode solicitar ao juiz a tomada das medidas adequadas para evitar ou interromper qualquer ação contrária a essa norma.

Pensando nas relações de consumo, o Código de Defesa do Consumidor, que é norteado pelo conceitos de proteção, informação adequada e prevenção, a LGPD 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, exceto naquelas situações em que o tratamento de dados pessoais ocorre estritamente para fins particulares e não econômicos.

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.

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 a cada dia que passa é possível interagir mais intensamente com essas novas tecnologias.

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 da internet das coisas.

Ante o exposto, tendo em vista a vigência da Lei nº 13.709/2018 (LGPD), a Sociedade Brasileira de Ortopedia e Traumatologia, através do seu setor Jurídico, em consideração aos seus parceiros e associados, vem a público fazer um breve resumo acerca das medidas necessárias para adequação de Hospitais e Clínicas à Lei Geral de Proteção de Dados.

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 tais dados para, por exemplo, direcionar conteúdos, controlar padrões de compras, vazar informações pessoais, enfim, promover uma ingerência indevida na esfera de privacidade dos titulares destes dados.

Neste contexto, a Lei nº 13.709/2018, dá especial relevância aos chamados dados pessoais sensíveis, sendo estes definidos em seu art. 5º, II como dados pessoais "*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.*"

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.

Sendo assim, é de suma importância que os Hospitais e Clínicas que prestam serviços de saúde, pública ou suplementar, 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.

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" a respeito da quantidade e qualidade dos dados que estão sendo coletados pela empresa atuante na área da saúde.

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

Neste sentido é importante observar:

1. Quais são os tipos de dados coletados pela empresa atuante na área da saúde;
2. Como é feito o tratamento de dados na empresa;
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 empresa; 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 pela empresa, como, também, a forma de tratamento, ou seja, de colheita, manejo e exclusão de tais dados pela empresa prestadora de serviços em saúde.

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

Sabendo quais dados a empresa coleta, o segundo passo é organizar tais dados, identificando a natureza de cada dado utilizado, ou seja, se são dados pessoais (art. 5º, I, LGPD); dados pessoais sensíveis (art. 5º, II, LGPD); dados anonimizados (art. 5º, III, LGPD); ou dados de crianças e adolescentes (art. 14, LGPD).

Com a referida organização há que se verificar se o tratamento desses dados, 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), segundo o qual o particular tem 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 os seus dados, 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.

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;
> 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 empresa 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 Arts. 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, 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.

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.

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

De acordo com o art. 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 o compartilhamento de seus dados, conforme dispõe o art. 7º, §5º, 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 (art. 9º, V, da LGPD). **Finalmente, tratando especificamente da área da saúde, é importante pontuar que o art. 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 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."

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, de modo transparente, para os particulares 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, 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, de 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.

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.

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 art. 52 da lei em comento, como é de se ver:

> "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:
> 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."

Portanto, como medida de prevenção, é imprescindível que as empresas se adequem à LGPD.

Do Encarregado (Data Protection Officer - DPO) e suas Funções

A Lei 13.709/18 (LGPD) determina, em seu artigo 5, VIII, 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 Art. 41 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
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 Art. 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 Art. 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 mandatório 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, 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 mitigar 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.

Proteção de Dados e Diretrizes do Conselho Federal de Medicina

A Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) não inaugura a tutela dos dados pessoais no ordenamento brasileiro. Antes, consolida e sistematiza princípios já presentes em nosso sistema jurídico, reforçando o dever de resguardar a intimidade, a privacidade e o sigilo profissional em saúde.

No âmbito das atividades médico-assistenciais, essa diretriz dialoga diretamente com as normas deontológicas e técnicas editadas pelo Conselho Federal de Medicina (CFM), de modo que a conformidade regulatória exige a leitura coordenada desses instrumentos.

Nesse contexto, já em 11 de julho de 2007, o CFM, atento ao avanço tecnológico e ao volume crescente de informações clínicas, editou a Resolução CFM nº 1.821/2007, que aprovou normas técnicas para a digitalização e o uso de sistemas informatizados na guarda e no manuseio de prontuários, autorizando, em condições específicas, a eliminação do papel e a troca segura de informações identificadas em saúde.

O ato normativo evidencia a preocupação prévia da autarquia com a confidencialidade, a integridade e a disponibilidade dos dados assistenciais, prevendo padrões de segurança compatíveis com a infraestrutura de chaves públicas brasileira.

A Resolução apoiou-se no Manual de Certificação para Sistemas de Registro Eletrônico em Saúde, desenvolvido pelo CFM em parceria com a Sociedade Brasileira de Informática em Saúde (SBIS), que instituiu níveis de segurança escalonados.

O Nível de Garantia de Segurança 1 (NGS1) estabelece requisitos robustos de controle de acesso, rastreabilidade e integridade.

Porém, a eliminação do suporte em papel demanda a utilização de certificados digitais da ICP-Brasil, nos termos da Medida Provisória nº 2.200-2/2001, e, por conseguinte, somente se perfaz integralmente no Nível de Garantia de Segurança 2 (NGS2), o qual especifica o emprego de certificação digital ICP-Brasil para

assinatura e autenticação, conferindo veracidade, não repúdio e validade jurídica aos registros eletrônicos.

Com a vigência da LGPD, tais diretrizes foram substancialmente reforçadas. Os princípios da finalidade, adequação, necessidade e segurança impõem que o tratamento de dados pessoais, especialmente os dados sensíveis de saúde, observe bases legais claras, controles técnicos e administrativos proporcionais ao risco e governança compatível com o ciclo de vida da informação clínica.

Em termos práticos, a adoção de sistemas certificados alinhados ao NGS2 e ao uso de certificados ICP-Brasil coaduna-se com a exigência de medidas de segurança aptas a proteger os registros contra acessos não autorizados, incidentes e adulterações, bem como a assegurar a rastreabilidade e a auditabilidade dos atos clínicos.

Dessa forma, o Manual de Certificação SBIS-CFM e a Resolução CFM nº 1.821/2007 permanecem como referência técnica e regulatória para o setor, funcionando de modo complementar à LGPD.

Enquanto a LGPD estabelece o regime jurídico de proteção de dados, as normas do CFM, em conjunto com o Manual de Certificação SBIS-CFM, definem requisitos operacionais e de segurança específicos para os sistemas de registro eletrônico em saúde.

A observância conjugada desses instrumentos não apenas legitima a substituição do papel por registros eletrônicos com valor jurídico, como também eleva o patamar de proteção do paciente, harmonizando sigilo médico, eficiência operacional e conformidade legal.

Conclusão

Como informado no tópico inicial, o presente documento tem como objetivo apresentar um resumo, ou seja, apresentar as 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 pela empresa.

A despeito disso, se espera que este breve documento, produzido com muito esmero pela **Sociedade Brasileira de Ortopedia e Traumatologia**, através do seu setor Jurídico, 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.