ABMES
Associação Brasileira de Mantenedoras de Ensino Superior

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 22/03/2021 | Edição: 54 | Seção: 1 | Página: 177
Órgão: Entidades de Fiscalização do Exercício das Profissões Liberais/Conselho Federal de Medicina

INSTRUÇÃO NORMATIVA CFM Nº 3, DE 3 DE MARÇO DE 2021

Institui a Política de Privacidade dos Dados das Pessoas Físicas no âmbito do Conselho Federal e nos Conselhos Regionais de Medicina

O CONSELHO FEDERAL DE MEDICINA, no uso das atribuições que lhe confere a Lei nº 3.268, de 30 de setembro de 1957, regulamentada pelos Decretos nº 44.045, de 19 de julho de 1958, e nº 6.821, de 14 de abril de 2009, e alterada pela Lei nº 11.000, de 15 de dezembro de 2014; e

Considerando as disposições contidas na Lei 13.709/18, referente a Lei Geral de Proteção de Dados;

Considerando o que dispõe a Instrução Normativa SGD/ME nº117, de 19 de novembro de 2020;

Considerando os estudos realizados pela Comissão instituída pela Portaria CFM nº 77/19;

Considerando serem os Conselhos de Medicina uma autarquia única, sendo os Conselhos Regionais subordinados ao Conselho Federal de Medicina, sobre tudo em questões institucionais e normativas, conforme artigos 1º e 3º da Lei 3.268/57, ressalvada a autonomia administrativa e financeira dos Conselhos Regionais de Medicina.

Considerando o decidido na reunião de diretoria do dia 03/ 03/21, resolve:

Art. 1º Instituir a Política de Privacidade dos Dados - PPD no âmbito do Conselho Federal e dos Conselhos Regionais de Medicina.

Art. 2º A PPD estabelece princípios e normas que devem nortear o tratamento de dados pessoais, físicos e digitais, no CFM e nos CRMS, a fim de garantir a proteção da privacidade de seus titulares, bem como define papéis e diretrizes iniciais para obtenção da gradual conformidade do CFM e nos CRMs ao previsto na Lei 13.709, de 2018.

Dos Conceitos

Art. 3º Para o disposto nesta Instrução Normativa, considera-se:

I - Política: definição de determinado objetivo da instituição e dos meios para atingi-lo;

II - Programa: conjunto de mecanismos e procedimentos administrados de forma integrada, reunidos em documento único, no qual são previstas ações articuladas e dinâmicas para atingir determinado objetivo;

III - Alta Administração: formada pela Administração Superior e pela Administração Executiva;

IV - Administração Superior: formada pela diretoria do CFM e dos Conselhos de Medicina;

V - Administração Executiva: formada pelos coordenadores e chefias do CFM e dos CRMS.;

VI - Autoridade Nacional de Proteção de Dados Pessoais: órgão vinculado à Presidência da República, ao qual caberá, dentre outras atribuições, fiscalizar a aplicação da LGPD nas entidades do poder público e aplicar sanções em caso de descumprimento de suas determinações;

VII - Princípio: norteamento para a atuação de conselheiros, funcionários, estagiários, terceirizados e de todos os que estabeleçam relação com o CFM e dos CRMS;

VIII - Gestão de Riscos: processo contínuo e técnico que consiste no desenvolvimento de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar eventos em potencial, capazes de comprometer o alcance dos objetivos organizacionais;

IX - Público interno: conselheiros, funcionários e colaboradores (estagiários e terceirizados);

X - Público externo: usuários dos serviços do CFM e nos CRMs e todos os que, de alguma forma, estabeleçam relações com a instituição;

XI - Privacidade: esfera íntima ou particular do indivíduo;

XII - Pessoa física: pessoa natural ou física;

XIII - Titular: pessoa física a quem se referem os dados pessoais objeto de tratamento;

XIV - Dado pessoal: informação relativa à pessoa física identificada ou identificável;

XV - 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;

XVI - Tratamento dos dados: qualquer atividade pertencente ao ciclo de vida dos dados pessoais;

XVII - Ciclo de vida dos dados: todas as etapas de manuseio dos dados, desde o surgimento destes na instituição até o respectivo descarte ou o arquivamento;

XVIII - Controlador: É a autoridade máxima do órgão, o que versa no Art. 5º, parágrafo VI da Lei 13.709/18, a quem competem as decisões referentes ao tratamento de dados pessoais;

XIX - Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

XX - Agentes de tratamento: o controlador e o operador;

XXI - 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).

Dos Princípios

Art. 4º Deverão ser considerados os seguintes princípios no tratamento de dados pessoais e em todas as ações relativas a ele:

I - boa-fé: convicção de agir com correção e em conformidade com o Direito;

II - finalidade: o tratamento dos dados deve possuir propósitos legítimos, específicos, explícitos e informados;

III - adequação: o tratamento dos dados deve ser compatível com a finalidade pela qual são tratados;

IV - necessidade: limitação do tratamento ao mínimo necessário para o alcance da finalidade, considerados apenas os dados pertinentes, proporcionais e não excessivos;

V - livre acesso: garantia aos titulares de consulta facilitada e gratuita sobre a forma e a duração do tratamento de seus dados pessoais bem como sobre a integralidade deles;

VI - 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 do respectivo tratamento;

VII - transparência: garantia aos titulares de informações claras, precisas e acessíveis sobre o tratamento de seus dados pessoais e sobre os agentes de tratamento;

VIII - segurança e prevenção: utilização de medidas técnicas e administrativas que garantam a proteção dos dados pessoais contra acessos não autorizados e a prevenção contra situações acidentais ou ilícitas que gerem destruição, perda, alteração, comunicação ou difusão desses dados;

IX - não discriminação: vedação de realizar o tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração de que os agentes de tratamento da instituição são responsáveis por este e adotam medidas eficazes para o cumprimento das normas de proteção dos dados pessoais.

Do Controlador e dos Operadores de Dados Pessoais

Art. 5º No CFM e nos CRMs, o Controlador é a autoridade máxima do órgão, o Operador considera-se como o ocupante da alta administração e o encarregado e o que será nomeado pela alta administração que realizará a comunicação entre a Autoridade Nacional de Proteção de Dados e o controlador.

§ 1º Deverá ser instituído um Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais para prestar suporte aos trabalhos da LGPD que será formado por uma equipe técnica e multidisciplinar, que desempenhe as funções jurídica, de segurança da informação e tecnológica, de comunicação interna e externa, de recursos humanos, de gestão documental e estratégica.

Art. 6º No CFM e nos CRMS, os operadores adjuntos são organizados em níveis:

I - Nível 1: os operadores são os coordenadores, chefias e seus subordinados;

II - Nível 2: os operadores são os supervisores e os coordenadores e os titulares dos núcleos permanentes;

III - Nível 3: os operadores são os componentes da Administração Executiva, os secretários, os conselheiros, os assessores de gabinete e os diretores de secretaria responsáveis pela gestão finalística, e os eventuais terceiros que atuem através de contratos firmados com o CFM e com os CRMS.

Parágrafo único. Deverá ser desenvolvida metodologia de controle do tratamento de dados pessoais que permita a revisão do fluxo dos dados realizado por um nível pelo nível imediatamente superior.

Art. 7º Compete ao Controlador:

I - instituir o Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais e definir as respectivas atribuições com base na LGPD;

II - designar o Encarregado pelas informações relativas aos dados pessoais;

III - fornecer as instruções para a política de governança dos dados pessoais e respectivos programas, dentre as quais:

a) o modo como serão tratados os dados pessoais no CFM e nos CRMs, a fim de que os respectivos processos sejam auditáveis;

b) a aplicação da metodologia de gestão de riscos no tratamento de dados;

c) a aplicação de metodologias de segurança da informação.

IV - determinar a capacitação dos operadores, para que atuem com responsabilidade, critério e ética;

V - verificar a observância das instruções e das normas sobre a matéria na instituição;

VI - comunicar à Autoridade Nacional e ao titular, em prazo razoável, a ocorrência de incidentes de segurança com os dados pessoais, que possam causar danos ou risco relevantes ao titular;

VII - incentivar a disseminação da cultura da privacidade de dados pessoais no CFM e nos CRMS;

VIII - determinar a permanente atualização desta Política e o desenvolvimento dos respectivos programas.

Art. 8º Compete aos operadores em todos os níveis:

I - documentar as operações que lhe cabem realizar durante o processo de tratamento de dados pessoais;

II - proteger a privacidade dos dados pessoais desde seu ingresso na instituição;

III - descrever os tipos de dados coletados;

IV - utilizar metodologia de coleta dos dados pessoais que considere a minimização necessária para alcançar a finalidade do processo;

V - capacitar-se para exercer as atividades que envolvam dados pessoais com eficiência, ética, critério e responsabilidade.

Do Encarregado pelos Dados Pessoais

Art. 9. O Controlador de cada Conselho é que nomeará o seu Encarregado pelos dados pessoais.

Art. 10. A função de Encarregado será exercida com o apoio do operador e do Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais e caberá ao Encarregado representá-lo perante ao Controlador e a Autoridade Nacional de Proteção de Dados.

Art. 11. Compete ao Encarregado:

I - ser o canal de comunicação entre a instituição e:

a) o titular de dados pessoais;

b) a Autoridade Nacional de Proteção de Dados Pessoais.

II - prestar esclarecimentos, realizar comunicações, orientar operadores e contratados sobre as práticas tomadas ou a serem tomadas para garantir a proteção dos dados pessoais;

III - determinar a publicidade da dispensa de consentimento para o tratamento de dados pessoais de cada Conselho, em conformidade com o previsto na LGDP;

IV - executar as atribuições a si determinadas pelo Controlador;

V - receber as reclamações dos titulares quanto ao tratamento de seus dados, respondê-las e tomar providências para que sejam sanados os desvios;

VI - deter amplo e sólido conhecimento sobre a legislação de proteção de dados pessoais e normas correlatas;

VII - deter conhecimentos técnicos sobre segurança e governança de dados;

VIII - realizar o atendimento dos titulares de dados pessoais internos e externos à instituição;

IX - manter a comunicação sobre o tratamento de dados pessoais com as autoridades internas e externas à instituição;

X - apoiar a implementação e a manutenção de práticas de conformidade do CFM e nos CRMS à legislação sobre o tratamento dedados pessoais;

XI - estabelecer campanhas educativas no órgão sobre o tratamento de dados pessoais;

XII - responder incidentes no tratamento de dados pessoais.

Das Normas para o Tratamento de Dados Pessoais no CFM e CRMS

Art. 12. O Conselho realizará o tratamento dos dados pessoais, necessário e imprescindível à garantia do interesse público e à execução de suas funções jurisidicionais e administrativas, à luz de suas atribuições legais.

Art. 13. O Consellho deverá publicar, de modo claro e atualizado, em lugar de fácil acesso e visualização em seu site, destinado à divulgação de informações sobre a privacidade de dados pessoais:

I - as informações previstas na lei dos conselhos que são cartoriais, judicantes e fiscalizatórias que fundamentam a realização do tratamento de dados pessoais na instituição;

II - a previsão legal, a finalidade e os procedimentos para tratamento de dados pessoais; [

III - a identificação do controlador e o contato deste;

IV - o nome do encarregado e o contato deste;

V - as responsabilidades dos operadores envolvidos no tratamento e os direitos do titular com menção expressa ao art. 18 da LGPD.

Art. 14. O tratamento dos dados pessoais deverá ser realizado durante todo o ciclo de vida destes na instituição:

I - acesso;

II - coleta;

III - avaliação:

IV - classificação;

V - armazenamento;

VI - controle;

VII - extração;

VIII - comunicação;

IX - distribuição:

X - difusão;

XI - eliminação;

XII - modificação;

XIII - processamento;

XIV - produção;

XV - recepção;

XVI - reprodução;

XVII - transferência;

XVIII - transmissão;

XIX - utilização.

Das Diretrizes

Art. 15. Para conformar os processos e os procedimentos dos Conselhos à Lei Geral de Proteção de Dados Pessoais, deverão ser consideradas as seguintes diretrizes:

I - levantamento dos dados pessoais tratados no CFM e nos CRMS;

II - mapeamento dos fluxos de dados pessoais no CFM e nos CRMS;

III - verificação da conformidade do tratamento com o previsto na LGPD;

IV - definição e publicação de programa de gerenciamento de riscos do tratamento de dados pessoais no CFM e nos CRMS;

V - revisão e atualização da política e dos programas de segurança da informação;

VI - definição de procedimentos e processos que garantam a disponibilidade, a integridade e a confidencialidade dos dados pessoais durante seu ciclo de vida;

VII - definição do modo de prestar as informações sobre o tratamento de dados pessoais;

VIII - revisão e adequação à LGPD dos contratos firmados no âmbito do CFM e nos CRMS;

IX - revisão e adequação à LGPD dos processos e procedimentos relacionados à área de saúde do prontuário e sigilo dos pacientes;

X - elaboração de Política de Tratamento de Dados Pessoais específica para dados relativos a crianças, jovens e idosos;

XI - definição do ciclo de vida das informações pessoais e da necessidade de consentimento para utilização de dados pessoais na parte administrativa do CFM e nos CRMS.

Das Disposições Finais

Art. 16. Esta Política deverá ser revisada e aperfeiçoada permanentemente, conforme sejam implementados os respectivos programas e constatada necessidade de novas previsões para conformidade do CFM e dos CRMS à LGPD.

Art. 17. As informações protegidas por sigilo continuam resguardadas pelos atos normativos a elas relacionados.

Art. 18. As omissões deste ato normativo serão dirimidas pela Administração Superior do CFM e nos CRMS.

Art. 19. Esta Instrução Normativa entra em vigor na data de sua aprovação.

MAURO LUIZ DE BRITTO RIBEIRO
Presidente do Conselho

DILZA TERESINHA AMBRÓS RIBEIRO
Secretária-Geral