CARTILHA

PROTEÇÃO DE DADOS PESSOAIS NO SETOR DE SAÚDE

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

OPICE BLUM
ACADEMY

ÍNDICE

1. O QUE É A LGPD?

A Lei 13.709/2018, conhecida como LGPD (Lei Geral de Proteção de Dados), entrou em vigor no dia 18 de setembro de 2020. Essa legislação conta com uma série de disposições para orientar e regular o tratamento de dados pessoais.

Há diversas normas e regulações setoriais que versam sobre privacidade e proteção de dados no Brasil, como o Código de Defesa do Consumidor, a Lei de Acesso à Informação, a Lei Geral de Telecomunicações, o Marco Civil da Internet, a própria Constituição Federal Brasileira e, no caso da saúde, as diversas normas setoriais da Agência Nacional de Saúde Suplementar (ANS), do Conselho Federal de Medicina (CFM), da Agência Nacional de Vigilância Sanitária (Anvisa), do Conselho Nacional de Saúde (CNS), entre outras.

2. O QUE SÃO DADOS PESSOAIS? E DADOS PESSOAIS SENSÍVEIS?

Dado pessoal é qualquer informação que possa identificar ou levar à identificação do seu titular, como dados cadastrais (nome, RG, CPF) e até mesmo dados comportamentais (preferências de navegação na internet, preferências de pesquisa em um navegador, o número identificador do seu celular e IP).

O **dado pessoal sensível** é uma categoria especial de dados pessoais, que, ante a possibilidade de ser utilizado para fins discriminatórios, está sujeito a regras mais rigorosas para seu tratamento. Os dados pessoais sensíveis são os dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou 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.

O legislador brasileiro adotou, portanto, o conceito amplo de saúde na LGPD - da mesma forma que fez o constituinte quando da sua definição nos artigos 6º e 196 da Constituição de 1988. Já o GDPR, regulamento europeu de proteção de dados, em seu Considerando de nº 35, traz definições mais específicas sobre o tema[1].

[1] Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test. Disponível em: https://gdpr-info.eu/recitals/no-35/. Acesso em 4 de abril de 2021.

3. QUAL É O OBJETO DE PROTEÇÃO DA LEI?

Ao proteger os dados pessoais, a LGPD objetiva tutelar os direitos fundamentais de liberdade e privacidade, bem como a autodeterminação informativa da pessoa natural.

Está em tramitação a Proposta de Emenda à Constituição nº 17/2019, que propõe modificar a redação do inciso XII do artigo 5º e acrescentar ao artigo 22 da Constituição Federal disposições específicas sobre proteção de dados pessoais, no que esse tema passará a figurar entre os direitos fundamentais do cidadão, fixando a competência privativa da União para legislar sobre a matéria. Em caso de aprovação, a proteção de dados passará a ser um direito fundamental expresso e garantido constitucionalmente.

Para saber mais sobre o tema, confira aqui o infográfico que preparamos sobre **"Aplicação da LGPD".** Clique aqui para acessar o de **"Autodeterminação informativa"**.

4. A QUEM SE DESTINA A LEI?

A Lei Geral de Proteção de Dados se destina a todas as pessoas naturais e jurídicas, de direito público ou privado, independentemente do meio, do país de sua sede ou do país em que estejam localizados os dados, desde que:

- O tratamento de dados seja realizado no Brasil;
- Os dados tenham sido coletados no território nacional; ou
- Ainda que ausente uma das situações anteriormente descritas, o tratamento tenha por objetivo a oferta ou fornecimento de bens ou serviços a indivíduos localizados no país.

Existem, no entanto, exceções sobre a aplicação da LGPD (art. 4º) ao tratamento de dados:

- Quando realizado por pessoa natural para fins exclusivamente particulares e não econômicos (ex: agenda telefônica usada para fins pessoais);
- Quando realizado para fins exclusivamente jornalísticos, artísticos e acadêmicos;
- Quando realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais;
- Quando os dados sejam provenientes de países que, por sua vez, ofereçam um nível de segurança jurídica adequado sobre esse tema (ex.: países da União Europeia) e apenas processados em território nacional, sem que haja qualquer intenção do agente brasileiro em compartilhar ou comunicar esses dados pessoais com outros agentes, exceto o agente que primariamente transmitiu a informação.

5. O QUE É TRATAMENTO DE DADOS PESSOAIS?

O conceito de tratamento de dados abrange qualquer operação feita com o dado pessoal, entre elas coleta, produção, recepção, classificação, utilização, o acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Nesse sentido, qualquer procedimento que usar dado pessoal será considerado tratamento e estará sujeito às regras previstas pela Lei Geral de Proteção de Dados Pessoais.

6. PRINCÍPIOS DA LGPD

A LGPD dispõe sobre uma série de regras para o tratamento de dados pessoais, sendo uma legislação essencialmente principiológica, já que estabelece os principais valores que deverão nortear a utilização dos dados pessoais pelos agentes de tratamento, sejam eles entidades públicas ou privadas.

Os princípios previstos são:

Finalidade: todo tratamento de dados pessoais deverá ter uma finalidade legítima, específica, explícita e informada ao titular do dado pessoal, justamente para que ele possa ter controle e ciência sobre o que está sendo feito com seu dado.

Adequação: o tratamento deverá ser adequado em relação às finalidades que foram informadas ao titular, de acordo com o contexto do tratamento.

Necessidade: todo tratamento de dados deverá ser o menos intrusivo possível, estando limitado ao mínimo necessário para o alcance de suas finalidades, envolvendo apenas os dados pertinentes, proporcionais e não excessivos para determinada atividade de tratamento.

Livre acesso: este princípio é uma garantia ao titular de que ele possa ter acesso, de forma fácil e gratuita, à integralidade de seus dados pessoais, bem como à forma e à duração do tratamento.

Qualidade dos dados pessoais: garante aos titulares a exatidão, clareza, relevância e atualização de seus dados, conforme necessidade e para o cumprimento da finalidade de seu tratamento, podendo os titulares corrigirem seus dados a qualquer tempo, por meio de procedimento facilitado e sem custos. Levando em consideração que os dados pessoais identificam seu titular, qualquer dado equivocado a respeito dele poderá implicar algum tipo de prejuízo.

Transparência: determina que o tratamento de dados pessoais seja feito com a maior transparência possível, garantindo ao titular informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes que o realizam, observados, contudo, os segredos comercial e industrial.

Segurança e prevenção: todo e qualquer agente de tratamento deverá aplicar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Prevenção: deverão sempre ser adotadas medidas para fins de prevenção da ocorrência de danos em virtude do tratamento de dados pessoais.

Não discriminação: nenhum dado pessoal poderá ser tratado em descrédito ou de forma injusta com relação ao seu titular ou, ainda, ser utilizado para discriminá-lo ou para outros fins ilícitos ou abusivos.

Responsabilização e prestação de contas: o agente de tratamento deverá ser capaz de demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das regras de proteção de dados pessoais.

7. POR QUE A ÁREA DA SAÚDE DEVE SE PREOCUPAR COM O TEMA?

Todas as áreas que lidam com dados pessoais no exercício de suas atividades precisam atentar para o tema da proteção de dados pessoais e conformidade com a LGPD. A área da saúde realiza reiteradamente tratamentos de dados sensíveis, o que traz a necessidade de adequação à LGPD de forma ainda mais determinante.

Isso quer dizer que, em um país onde os beneficiários da saúde suplementar ultrapassam 47,6 milhões, de acordo com o número mais recente, de dezembro de 2020, e se realizaram 1,62 bilhão de procedimentos em 2019, conforme dados da Agência Nacional de Saúde (ANS)[1], ficam evidentes o enorme fluxo e volume de dados pessoais envolvidos. E isso sem contar o Sistema Único de Saúde, que também deverá se adequar às disposições da LGPD, já que as regras nela previstas também se aplicam ao Poder Público.

Outro aspecto que demanda atenção é o fato de que o setor da saúde, há algum tempo e cada vez mais, tem buscado a adoção de diversas ferramentas tecnológicas, servindo-se da Inteligência Artificial e do Big Data, por exemplo, para avançar em pesquisas, reduzir custos de tratamento, prever epidemias e aumentar a eficiência do atendimento, processos esses que intensificam ainda mais o tratamento de dados pessoais.

Assim, é inegável a necessidade do setor de saúde, que já dispõe de uma série de regulações e normas setoriais próprias também envolvendo o sigilo e confidencialidade das informações dos pacientes e usuários do sistema de saúde, de se atentar para a privacidade e proteção de dados pessoais dos titulares, conforme regramento trazido pela Lei Geral de Proteção de Dados Pessoais.

[1] Disponível em: http://www.ans.gov.br/perfil-do-setor/dados-gerais. Acessado em 06/04/2021.

8. EM QUAIS MOMENTOS A ÁREA DA SAÚDE UTILIZA DADOS PESSOAIS?

Apesar de ser intuitivo o fato de os dados pessoais permearem toda a cadeia da saúde, exemplificamos abaixo alguns momentos em que os dados pessoais são tratados nesse ecossistema e que, portanto, merecem especial atenção:

8.1. Precificação de plano e dos serviços de saúde

A ANS determina[2] que, para a contratação de qualquer plano de saúde, o contratante apresente a chamada **Declaração Pessoal de Saúde (DPS)**, por meio da qual deverá informar sua condição atual de saúde e eventuais doenças pré-existentes para que a operadora possa então verificar a necessidade de aplicação de Carência, Agravo ou Cobertura Parcial Temporária.

Nessa operação, todas as informações constantes na DPS são consideradas dados pessoais, pois dizem respeito a uma pessoa natural, nos termos do artigo 5º, I, da LGPD. Da mesma forma, também podem conter dados pessoais sensíveis referentes à saúde do beneficiário e dos seus dependentes.

Quando da contratação de planos de saúde, vale destacar a redação do artigo 11, §5º, LGPD, na qual ficou determinado que "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."

[2] Artigo 9º da RN 162 da ANS

Da leitura isolada da redação do artigo 11, §5º, da LGPD, pode surgir a interpretação de que a LGPD imporia proibição terminal de que dados de saúde sejam utilizados para cálculo de risco. Entretanto, ao fazer a devida interpretação sistemática do dispositivo frente ao ordenamento jurídico, sobretudo em observância ao que dispõe a Súmula Normativa nº 27/2015 da ANS, a qual serviu de inspiração à norma em questão, afasta-se essa compreensão.

Nesse contexto, cabe destacar que o contrato de seguro é classificado como aleatório, por estar presente a chamada "álea", termo que diz respeito ao risco de prejuízo. O risco está presente uma vez que a prestação e contraprestação dos serviços são estipuladas no momento da contratação. Entretanto, a prestação da seguradora está condicionada a evento futuro e incerto; cite-se, como exemplo, necessidade de exames, necessidade de procedimentos cirúrgicos, internação, eventos esses que, obviamente, implicam risco financeiro.

Portanto, é inerente ao contrato de seguro o cálculo de risco, notadamente porque isso poderá pautar o preço da contraprestação a ser quitada pelo segurado. A ANS, inclusive, reconhece – por meio da Súmula Normativa nº 27/2015 – a existência de mecanismos legais de mitigação de riscos por parte das operadoras de planos privados de assistência à saúde, por meio da aplicação de carência, cobertura parcial temporária ("CPT") e agravo.

Diante disso, a redação dada pela ANS à Súmula Normativa nº 27/2015, bem como o entendimento adotado pelo legislador, amplamente inspirado na referida normativa, não extinguiram a análise de risco com base em dados de saúde, mas somente vedaram a seleção de risco que possa acarretar na exclusão de segurados ou na não contratação com pessoas que sejam classificadas como de risco alto.

Com efeito a ANS não pretendeu com a Súmula Normativa nº 27/2015 excluir a análise de riscos, mas somente garantir **que não haja restrições discriminatórias, tanto no momento da contratação, quanto no decorrer do contrato, ou seja, seleção com base em análise de risco.**

8.2. Atendimento de pacientes

O atendimento do paciente traz situações nas quais o tratamento de dados ocorre. De acordo com pesquisa do Comitê Gestor da Internet (CGI), realizada em 2019, 85% dos enfermeiros e 92% dos médicos usam o computador para atendimento a pacientes.[3]

8.2.1. Hospitais (Ambulatório e PS):

Hospitais, em circunstâncias emergenciais ou não, utilizam dados pessoais dos pacientes para identificá-los, bem como para aferir sua situação de saúde por meio da anamnese, procedimento médico em que se verificam os parâmetros vitais relacionados à pressão arterial, temperatura corporal, glicemia, reflexos neurais, nível de consciência e outros condizentes com o contexto clínico, histórico medicamentoso, entre outras informações, conforme artigo 51 da Resolução 2.056 do Conselho Federal de Medicina (CFM).

Todos esses dados são registrados em um documento de extrema importância para o histórico médico do paciente, seja no ambiente hospitalar, seja em clínicas, que é o prontuário médico, conceituado pelo artigo 1º da Resolução 1.638/2002 do CFM como "documento único constituído de um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter

[3] Disponível em https://cetic.br/media/analises/tic_saude_2019_coletiva_de_imprensa.pdf. Acesso em 06.04.2021.

legal, sigiloso e científico, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo."

Nesse sentido, o prontuário médico é documento sigiloso[4], não podendo ser compartilhado com ninguém sem que haja o consentimento esclarecido do paciente[5]. O tempo para sua guarda deverá respeitar o prazo de 20 anos, contados a partir do último registro[6], se em suporte físico. Quando em suporte digital, a guarda deverá ser permanente[7], não podendo haver o descarte da via física se o estabelecimento não tiver o nível 2 de segurança da informação (N2SG) nos termos do item 8.1.1 do Manual de Certificação para Sistemas de Registro em Saúde[8].

A Lei nº 13.787/2018 estabeleceu regras específicas para a digitalização do prontuário eletrônico, seu armazenamento e exclusão, inclusive de sua versão em papel. Sendo assim, conforme previsto em seu artigo 3º, os documentos originais poderão ser eliminados após a digitalização se cumpridos os requisitos do artigo 2º, passando por aprovação depois de análise obrigatória da Comissão de Avaliação, que verificará a integridade das cópias. Por fim, em seu artigo 6º, estabelece que, decorrido o prazo de 20 anos, ambos os formatos de prontuário poderão ser eliminados.

Não se pode esquecer, ainda, que os hospitais também lidam com os dados pessoais de visitantes e acompanhantes, os quais também deverão ser tratados em observância às regras previstas na Lei Geral de Proteção de Dados Pessoais.

---

4 Definido pela Resolução 1.638/2002 do CFM
5 Art. 1º da Resolução 1.605/2000 do CFM
6 Artigo 8º da Resolução 1821/2007 do CFM
7 Artigo 7º da Resolução 1821/2007 do CFM
8 NGS2 - categoria constituída por S-RES que viabilizam a eliminação do papel nos processos de registros de saúde. Para isso, especifica a utilização de certificados digitais ICP-Brasil para os processos de assinatura e autenticação. Para atingir o NGS2, é necessário que o S-RES atenda aos requisitos já descritos para o NGS1 e apresente ainda total conformidade com os requisitos especificados para o Nível de Garantia 2.

8.2.2. Laboratórios

A medicina diagnóstica e de medicamentos manipulados também deve ser incluída no rol de agentes do sistema de saúde que realizam operações de tratamento de dados pessoais. Nesses casos, os dados pessoais podem ser utilizados para identificação do paciente e dos demais profissionais de saúde envolvidos, para verificação dos exames e procedimentos solicitados pelo médico responsável ou, ainda, para o medicamento que deve ser manipulado.

Em relação aos exames radiológicos, destaca-se:

"(...)nos casos de exames realizados em unidades radiológicas sem vínculo com estabelecimento hospitalar, onde o paciente não procura recebê-los para mostrá-los ao médico solicitante, permanece a responsabilidade de guarda, pois foram produzidos em decorrência de suas atividades específicas, devendo ser observado o definido na Resolução CFM nº 1.821/07. O dever de guarda em relação ao exame radiológico cessa com a sua retirada pelo paciente, no entanto deve ficar arquivado uma via do laudo emitido. Uma possibilidade seria a remessa pelos correios ao paciente ou responsável legal, mediante aviso de recebimento. A entrega pessoal dos exames deve ser feita mediante protocolo."

[9] Consulta CFM Nº 4.728/08 – Parecer CFM Nº 10/09

8.2.3. Clínicas e consultórios médicos

Grande parte dos atendimentos a pacientes ocorre em clínicas e consultórios médicos, nos quais diferentes profissionais estão envolvidos e são responsáveis pelo tratamento dos dados pessoais e sensíveis dos pacientes. Nesse sentido, esses locais de atendimento deverão adotar medidas para garantir que os dados sejam tratados de forma adequada, respeitando os princípios trazidos pela LGPD, em especial os da finalidade, necessidade e transparência, de modo que sejam utilizados apenas os dados necessários para o alcance de fins específicos e informados ao titular, sempre em respeito à sua privacidade e dentro das hipóteses legais autorizadoras do tratamento.

Adicionalmente, as clínicas e os consultórios deverão intensificar as preocupações relacionadas à manutenção da confidencialidade dos documentos do paciente, principalmente seu prontuário médico, garantindo que eles sejam armazenados de forma segura e acessados somente pelos profissionais que de fato precisem ter conhecimento das informações clínicas do paciente.

8.2.4. Telemedicina

O uso da telemedicina é recurso, há tempos, bastante incentivado em razão dos diversos benefícios que proporciona para a gestão da saúde. Como exemplo, temos a redução de pessoas buscando atendimento em hospitais nas situações em que esse atendimento possa ocorrer de forma remota, evitando a exposição de pacientes a riscos hospitalares, bem como deslocamentos e custos desnecessários, além de permitir economia de tempo do paciente e dos próprios profissionais de saúde.

Nesse sentido, é evidente a melhoria na experiência do paciente e os ganhos para os profissionais e sistema e saúde como um todo.

A experiência do paciente é cada vez mais considerada para equalização dos custos na saúde. A confiança no profissional de saúde que presta o atendimento, o tratamento que é ministrado e o conforto depositado nos mecanismos de interação com o médico são fatores primordiais para fazer com que esse paciente não procure outro profissional, que poderá prescrever outros exames, procedimentos e tratamentos, elevando assim o custo para o sistema de saúde.

A telemedicina surgiu, em meados dos anos 80, no contexto de aproximar especialistas, que geralmente estão nos grandes centros, de pessoas que não têm condições de se consultar com tanta facilidade e que geralmente estão nas periferias. No Brasil, a telemedicina cresce cada vez mais e, desde 2001, já há regulação sobre a utilização de meios televisuais para o atendimento de pacientes e transmissão de dados, a exemplo da Resolução nº 93/2001 do CREMESP (Telerradiologia) e Resolução nº 1.643/2002 do CFM que trata sobre a utilização da telemedicina.

Sobre a Resolução nº 1.643/2002 é importante ressaltar que ela traz o conceito de telemedicina como a "utilização de metodologias interativas de comunicação audiovisual e de dados, com o objetivo de assistência, educação e pesquisa em Saúde." Assim, é preciso ter em mente que a telemedicina não se destina somente ao atendimento do paciente.

Interessante acrescentar que a referida Resolução não é específica no que diz respeito à modalidade de telemedicina que seria permitida, considerando que ela pode ocorrer para consultas de rotina ou até mesmo cirurgia.

Com o passar do tempo, as interpretações do próprio Conselho Federal de Medicina se restringiam a permitir somente a teleorientação, teleconsulta e teleinterconsulta. Em 2018, apesar de ter sido aprovada nova resolução (CFM nº 2227/2018), que aumentou o escopo da telemedicina permitida no Brasil para abarcar inclusive a telecirurgia, tal resolução foi suspensa para maiores discussões do setor.

Em razão da disseminação do coronavírus, o Ministério da Saúde editou a Portaria 467/2020, que autoriza o telemonitoramento e o telediagnóstico durante o período extraordinário da pandemia, além das modalidades que já eram liberadas. Paralelamente, foi aprovada a Lei 13.989/2020, que teve origem no Projeto de Lei 696/2020, permitindo a utilização da telemedicina para qualquer modalidade durante o período de contenção da pandemia, restando ao CFM a obrigação de regular posteriormente.

Apesar dos benefícios da utilização da telemedicina, não podemos esquecer que a utilização de tecnologia, aliada ao tratamento de dados pessoais de saúde, que podem ser, inclusive, de pessoas em situação de vulnerabilidade, como idosos e crianças, acaba por tornar a operação arriscada, demandando cuidados adicionais, de cunho técnico e administrativo, sobretudo de treinamento dos profissionais, para a garantia da privacidade dos titulares de dados pessoais.

Há legislações estrangeiras que já tratam o tema com maturidade. Entre elas está o *Health Insurance Portability and Accountability Act* (HIPAA) norte-americano. Em relação à telemedicina, debruçou-se em desenvolver orientações para sua proteção por meio das ePHI (*Electronic Protected Health Information*), com sua aplicação a qualquer profissional médico ou organização que adote tais práticas de atendimento remoto, determinando que:

i) somente pessoas autorizadas devem acessar a ePHI;

ii) deve ser implementado um sistema de comunicação segura para proteger a integridade da ePHI;

iii) deve ser implementado um sistema de monitoramento de comunicações contendo ePHI, de modo a prevenir vazamentos maliciosos ou acidentais.

8.3. Pesquisa Clínicas

Segundo a Agência Nacional de Vigilância Sanitária (Anvisa), pesquisa clínica pode ser conceituada como "(...) estudos realizados com humanos para medir os parâmetros de segurança e eficácia de novos medicamentos, sendo essencial para a chegada de novas alternativas terapêuticas no mercado[10]."

A Resolução nº 466/2012 do Conselho Nacional de Saúde (CNS) disciplina a atividade de pesquisa clínica, dispondo, entre outras questões, sobre a necessidade de consentimento livre e esclarecido da pessoa que pretende participar do processo de pesquisa, cabendo ao pesquisador, além de elaborar o termo de consentimento livre e esclarecido[11], observar todo o rígido processo de coleta e gerenciamento desse consentimento[12].

Assim, além dos dados para identificação do participante, ainda que sua identificação seja reduzida a determinado código, as empresas que desenvolvem esse tipo de atividade também possuem todo o histórico de efeitos e condições adversas da pesquisa no voluntário, incluindo seu estado clínico antes do início do procedimento de pesquisa, para o que deverá observar não somente as normas regulatórias específicas para o tema, mas também a LGPD.

Necessário esclarecer que não se deve confundir o TCLE (Termo de Consentimento Livre e Esclarecido) do consentimento previsto como base legal autorizadora para o tratamento de dados pessoais e sensíveis pela LGPD. Por serem instrumentos com origens e objetivos diferentes, eles devem ser aplicados em conjunto e sempre que necessário, cada um de acordo com os requisitos específicos trazidos por seus respectivos ordenamentos.

10 Disponível em http://portal.anvisa.gov.br/pesquisa-clinica

11 Item XI.2, b, da Resolução 466/2012 da Anvisa

12 Item IV da Resolução 466/2012 da Anvisa

8.4. Farmácias

As farmácias também detêm ampla base de dados de seus consumidores, não somente pelos eventuais cadastros voluntários que são feitos por eles, mas também porque entre as atividades do farmacêutico está o estabelecimento de "perfil farmacoterapêutico no acompanhamento sistemático do paciente, mediante elaboração, preenchimento e interpretação de fichas farmacoterapêuticas."[13]

Além disso, por obrigação regulatória, prevista no artigo 52, §1º, da Resolução 44/2009 da Anvisa, é obrigação do farmacêutico averiguar a receita para o fornecimento de medicamentos sujeitos à prescrição, o que demanda a identificação do paciente e do medicamento solicitado.

Além disso, é atividade permitida ao farmacêutico pela Resolução nº 44/2009 em seu artigo 63, §1º que "para subsidiar informações quanto ao estado de saúde do usuário e situações de risco, assim como permitir o acompanhamento ou a avaliação da eficácia do tratamento prescrito por profissional habilitado, **fica permitida a aferição de determinados parâmetros fisiológicos e bioquímicos do usuário, nos termos e condições desta Resolução"** (grifos nossos), o que depende, nos termos da Resolução, de consentimento expresso do usuário (art. 64, §1º).

Nesse sentido, além de dados clínicos e histórico de medicamentos, há situações em que as farmácias podem solicitar a realização de cadastros com informações como CPF e plano de saúde ao qual o consumidor está vinculado, o que tem sido objeto de estudos e alinhamentos normativos, conforme será analisado no item 21 desta cartilha.

Ademais, o Estado de São Paulo promulgou, em 1º de dezembro de 2020, a Lei 17.301/2020 que estabelece regras específicas para a coleta de CPF nas farmácias, exigindo que o estabelecimento explique ao consumidor os motivos da coleta, além de disponibilizar informação específica nos locais de passagem frequente.

[13] Art. 13º, V, da Lei nº 13.021/2014, que dispõe sobre o exercício e a fiscalização das atividades farmacêuticas

9. TRATAMENTO DE DADOS DE SAÚDE PELO PODER PÚBLICO

Sobre o tratamento de dados pessoais, é preciso considerar o papel desempenhado pelo Poder Público, que tem em suas mãos a incumbência de governar sobre diversos assuntos, mas principalmente sobre a saúde pública e, para isso, necessita de informações para que possa desenvolver e implementar políticas públicas eficientes.

Verifica-se que o país está cada vez mais caminhando para a utilização da tecnologia na gestão da saúde, o que se mostra relevante, mas que, por outro lado, demanda maturidade do Poder Público para que se tenha estrutura adequada para garantir a segurança dos dados pessoais. Neste contexto, citamos como exemplo o Conjunto Mínimo de Dados[14] e a Rede Nacional de Dados em Saúde.

Em relação ao Conjunto Mínimo de Dados, as empresas de atenção à saúde como hospitais, clínicas, operadoras de saúde, entre outras, devem compartilhar uma série de informações cadastrais e de saúde dos seus pacientes com o Ministério da Saúde, para que esse, na posse de tais dados, possa verificar as necessidades da saúde pública e elaborar políticas públicas capazes de atender a população de forma eficiente.

Além disso, para tornar mais eficaz a utilização de dados na saúde, bem como para diminuir a assimetria de informação nesse ecossistema, foi criada a Rede Nacional de Dados em Saúde, que une todos os registros eletrônicos de saúde em uma mesma base de dados e que está acessível a qualquer profissional ou empresa que tenha necessidade de consultá-la, desde que haja o consentimento do paciente para tanto.

Em razão da pandemia de Covid-19, é necessário que o Poder Público tenha controle sobre a evolução dos casos de contaminação e óbito, o que demanda manuseio de grande massa de dados pessoais de saúde, sobretudo, em decorrência da obrigação legal de notificar as autoridades sobre casos de contágio (vide Lei Federal nº 6.259 de 30 de outubro de 1975 e Lei 13.979/2020).

[14] Art. 13º, V, da Lei nº 13.021/2014, que dispõe sobre o exercício e a fiscalização das atividades farmacêuticas

10. TRATAMENTO DE DADOS DE SAÚDE DE COLABORADORES

Além dos dados pessoais dos pacientes e demais usuários que utilizam os serviços de saúde, todas as instituições e empresas, públicas ou privadas, atuantes nesse ramo, também deverão se preocupar com os dados dos seus colaboradores (médicos, enfermeiros, terapeutas, atendentes e todos os demais profissionais envolvidos no sistema de saúde).

Nesse cenário, os dados pessoais dos colaboradores geralmente são tratados para fins de admissão, registro do vínculo empregatício e compartilhamento dos dados com instituições como o Ministério do Trabalho e da Fazenda, em cumprimento a obrigações legais. Como exemplos, temos os registros de ponto – que, muitas vezes, são realizados com registro biométrico para evitar fraudes na marcação; dados de saúde ocupacional, que implica a gestão de exames médicos admissionais, periódicos e demissionais; dados de pagamento, benefícios, dependentes, entre outros necessários para o desenvolvimento da relação empregatícia.

Importante destacar ainda que é obrigação dos empregadores zelar pela saúde dos seus funcionários e, para tanto, têm responsabilidade legal sobre o controle do ambiente de trabalho, garantindo que seja salubre.

Assim, considerando cenários como o da pandemia Covid-19, existe fundamento para que as empresas solicitem informações pertinentes para auxiliar na preservação de ambiente seguro, especialmente tomando em conta o disposto no artigo 3º, III, da Lei 13.979/20, no qual há disposição sobre a realização compulsória de exames médicos, testes laboratoriais, coleta de amostras clínicas, vacinação ou tratamentos médicos, dentro dos estritos limites legais, em situações específicas.

No entanto, ainda que seja importante manter ambiente seguro dentro das empresas, é recomendável cuidado na abordagem aos indivíduos potencialmente contaminados (garantindo o atendimento dos princípios da finalidade, adequação, necessidade, ausência de discriminação, entre outros), em especial com a adoção de medidas que possam ser consideradas discriminatórias.

É recomendável que essa abordagem seja conduzida por profissionais da área da saúde, haja vista a coleta de informações de estado de saúde do indivíduo. Não sendo possível, sugerimos que o representante do Departamento de Recursos Humanos realize a coleta dos dados, os quais deverão ser tratados de forma segura e restrita. Após o entendimento das informações acima, em havendo suspeita de contaminação, sugerimos que sejam seguidos os protocolos oficiais disponibilizados pelas autoridades de saúde locais.

Para mais informações sobre essa questão, sugerimos que seja verificada a cartilha intitulada "**COVID-19: Tratamento de dados pessoais no ambiente corporativo**", também preparada pelo Opice Blum, Bruno e Vainzof Advogados Associados.

11. TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES

O artigo 14 da LGPD prevê que o tratamento de dados pessoais de crianças e adolescentes deva ser realizado no seu melhor interesse, estabelecendo, contudo, regimes diversos para quando o tratamento se referir a dados desses indivíduos.

Segundo o artigo 2º do Estatuto da Criança e Adolescente (Lei nº 8.069/90), considera-se criança o indivíduo com até 12 anos de idade incompletos. A LGPD prevê em seu artigo 14, §1º, que o tratamento deverá, obrigatoriamente, contar com o consentimento de, pelo menos, um dos pais ou do responsável legal.

Essa exigência pode trazer dificuldades práticas, já que, em alguns casos, os estabelecimentos que lidam com dados pessoais de crianças, sobretudo em se tratando de hospitais, estão atuando com situações emergenciais, nas quais não haverá tempo para a coleta prévia do consentimento dos pais. Para ocasiões como essa, a lei traz uma exceção, que permite eventual tratamento de dados pessoais de crianças sem o consentimento exigido. O objetivo é garantir a proteção da vida da criança. Nesse caso, os dados podem ser utilizados uma única vez e sem armazenamento. Mas, sob hipótese alguma, podem ser repassados a terceiros.

12. QUANDO O TRATAMENTO É PERMITIDO?

Em regra, o tratamento de dados sensíveis somente é permitido se for verificada alguma das seguintes situações:

- Havendo **consentimento do titular** (Ex.: paciente que consente com o compartilhamento de seus dados; voluntário que consente em participar de pesquisa clínica);

- Para o **cumprimento de obrigação legal ou regulatória pelo controlador** (Ex.: guarda de dados registrados em prontuário físico por 20 anos a partir do último registro, conforme Resolução CFM 1.639/2002 e Lei nº 13.787/2018);

- **Pela Administração Pública, para a execução de políticas públicas** (Ex.: dados de epidemia para desenvolvimento de política de prevenção ou combate à determinada doença);

- **Para a realização de estudos por órgãos de pesquisas** (com anonimização dos dados sempre que possível) (Ex.: dados para pesquisa da eficácia de determinado medicamento);

- **Para o exercício regular de direito em contratos e processos judiciais, administrativos ou arbitrais** (Ex.: celebração de contrato para a prestação de serviços médico-hospitalares ou de planos individuais; ou na defesa da instituição em eventual ação judicial proposta pelo beneficiário ou para arguir eventual fraude na Declaração Pessoal de Saúde junto à ANS);

- **Para a proteção da vida ou incolumidade física** do titular ou terceiro;

- **Para a tutela da saúde**, em procedimento realizado por profissionais da área de saúde, serviços de saúde ou autoridade sanitárias;

- **Para prevenção à fraude e garantia de segurança do titular** (Ex.: nos casos de escaneamento de íris para identificação ou circuito interno de TV que filma UTIs).

É importante notar que as bases legais que autorizam o tratamento de dados de saúde não abarcam a execução de contrato (havendo apenas a previsão para o exercício regular de direitos em contrato, como acima destacado), o legítimo interesse (havendo a prevenção à fraude e segurança do titular) e proteção do crédito.

13. E SE O TRATAMENTO NÃO SE ENCAIXAR EM NENHUMA DAS HIPÓTESES PREVISTAS NA LEI?

Segundo a redação dos artigos 7º e 11º da LGPD, o tratamento somente pode ser realizado nas hipóteses autorizadoras previstas nesses artigos. Sendo assim, se o tratamento não se encaixar em nenhuma dessas hipóteses, o agente de tratamento deverá repensar a atividade para que possa se amoldar a alguma hipótese de autorização ou **deixar de realizar a operação.**

14. O SETOR DA SAÚDE JÁ POSSUI NORMAS DE PROTEÇÃO DE DADOS PESSOAIS?

Já foi dito que o setor da saúde possui diversas normas pertinentes que consideram o titular do dado pessoal em sua privacidade. Dentre elas, podemos citar:

- **Lei nº 8.078/90**, o Código de Defesa do Consumidor, regulamenta os bancos de dados consumeristas;

- **Lei nº 12.965/2014**, Marco Civil da Internet ("MCI"), que estabeleceu direitos, limites e obrigações de usuários e serviços de Internet, inclusive plataformas e aplicativos de saúde. A lei trata especificamente de questões ligadas ao uso de dados pessoais, tais como a necessidade de consentimento prévio, livre, específico e informado dos usuários, porventura pacientes;

- **Decreto nº 8.771/16**, que regulamentou aspectos do MCI, inclusive sobre o uso de dados pessoais, estabelecendo limites, como a obrigação de coletar dados somente para finalidade determinada, apenas na quantidade e nos tipos necessários para atingir esse propósito, devendo esses serem cancelados ao atingir a finalidade, caso não haja outra base legal para mantê-los.

• **Resolução nº 1.821/2007 do CFM**, que dispõe sobre o prontuário eletrônico de dados médicos, considerados sensíveis;

• **Resolução Normativa nº 305/2012 da ANS**, que estabeleceu o Padrão obrigatório para Troca de Informações na Saúde Suplementar – Padrão TISS – dos dados de atenção à saúde dos beneficiários de Plano Privado de Assistência à Saúde;

• **Resolução Normativa nº 162/2007 da ANS**, que trata sobre a declaração pessoal de Saúde;

• **Resolução nº 1.605/2000 do CFM,** que determina o compartilhamento de dados pessoais mediante consentimento do titular dos dados;

• **Resolução nº 1643/2002 do CFM**, que trata sobre a telemedicina e a necessidade de sigilo dos dados do paciente;

• **Portaria nº 467/2020 do Ministério da Saúde**, que trata sobre a utilização da telemedicina no período de controle da pandemia do coronavírus e trata sobre obrigação de sigilo dos dados do paciente;

• **Resolução nº 466/2012 do Conselho Nacional de Saúde** , que trata sobre a pesquisa clínica e do consentimento livre e esclarecido;

• **Resolução nº 44/2009 da Anvisa**, que trata sobre boas práticas farmacêuticas para o controle sanitário do funcionamento, da dispensação e da comercialização de produtos e da prestação de serviços farmacêuticos em farmácias e drogarias e dá outras providências.

• **Lei nº 13.021/2014**, que dispõe sobre o exercício e a fiscalização das atividades farmacêuticas e trata do preenchimento de fichas farmacoterapêuticas com dados pessoais, que podem ser considerados dados consumeristas, e dados pessoais sensíveis, como os que revelam alguma característica fisiológica de pacientes;

• **Lei nº 13.787/18**, que dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.

• **Lei nº 13.989/20**, que dispõe sobre o uso da telemedicina durante a crise causada pelo novo coronavírus.

Fica claro assim que, na maior parte das vezes, a LGPD não será o único dispositivo legal aplicado ao caso concreto, devendo haver interpretação harmônica e compatível com as demais normas legais e regulatórias aplicáveis ao setor.

15. PROTEÇÃO DE DADOS E AS TECNOLOGIAS NA ÁREA DA SAÚDE

Os princípios e as obrigações trazidos pela LGPD, inspirada no GDPR, permitem a utilização de conceitos como *Privacy by Design* e *Privacy by Default*, os quais demandam que a privacidade seja considerada desde a concepção do produto e como padrão. Sendo assim, os programadores ao pensar em soluções para qualquer área de negócio, e especialmente na área da saúde, terão de olhar para a privacidade como valor nuclear e intrínseco ao produto ou serviço.

Para atender a esses princípios, é recomendável que todos os novos projetos sejam avaliados por meio do Relatório de Impacto à Proteção de Dados, em que a empresa deverá relatar no mínimo:

a) Descrição da natureza, escopo, contexto e finalidades do tratamento, bem como descrição dos dados pessoais tratados;
b) Necessidade, proporcionalidade de interesses (empresa/titular dos dados);
c) Possíveis riscos envolvidos ao titular dos dados pessoais;
d) Medidas para mitigação de riscos, bem como boas práticas;
e) Parecer do Encarregado a respeito da operação;
f) Verificação dos riscos residuais após a aplicação das medidas mitigadoras;
g) Plano de ação ou assinatura de gestor que aceitará o risco residual.

Portanto, atividades como telemedicina, telerradiologia e ultrassom realizadas a partir de ferramentas disponibilizadas em dispositivos móveis como celulares, *analytics* em saúde ou Inteligência Artificial deverão ser implementadas e operadas com vistas à privacidade do titular do dado pessoal, com medidas técnicas e administrativas embarcadas para que sejam garantidas a privacidade e a segurança do titular do dado pessoal, desde a concepção do produto.

15 O GDPR (General Data Protection Regulation) é a lei da União Europeia que versa sobre a privacidade e o tratamento de dados pessoais, a qual inspirou fortemente a legislação brasileira.

16. COMPARTILHAMENTO DE DADOS SENSÍVEIS COM TERCEIROS

A LGPD determina no artigo 11, §3º, que o compartilhamento de dados sensíveis poderá ser objeto de vedação ou regulamentação específica pela Autoridade Nacional de Proteção de Dados, trazendo, entretanto, regras específicas a respeito do compartilhamento de dados pessoais sensíveis de saúde entre controladores para obtenção de vantagem econômica.

No mesmo sentido, o artigo 11, §4º, veda o compartilhamento de dados de saúde entre controladores para obtenção de vantagem econômica, exceto quando for necessário para prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, sempre em benefício dos interesses dos titulares de dados.

A portabilidade e as transações financeiras e administrativas que necessitem de compartilhamento de dados pessoais de saúde também o justificam nos termos do artigo 11, §4º, I e II, da LGPD, podendo ser adotada a portabilidade entre planos de saúde ou a necessidade de faturamento de procedimentos entre um hospital credenciado e o respectivo plano de saúde.

A CNSaúde (Confederação Nacional de Saúde), em parceria com a ANS e outras instituições, desenvolveu Código de Boas Práticas que dedica, em sua segunda parte, atenção especial ao compartilhamento de dados pessoais de saúde nesse contexto. Saiba mais aqui.

17. OS TITULARES TÊM DIREITOS SOBRE SEUS DADOS?

É muito importante esclarecer que a Lei Geral de Proteção de Dados, além de trazer obrigações para os controladores e operadores, traz direitos aos titulares dos dados, como:

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 o disposto na Lei;

V - **portabilidade** dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;

VI - **eliminação** dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da Lei;

VII - **informação** das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de **não fornecer consentimento** e sobre as consequências da negativa; e

IX - **revogação** do consentimento, nos termos do § 5º do art. 8º desta Lei.

O titular tem direito de solicitar, ainda, a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. Nesse sentido, sempre que solicitado, o titular poderá receber informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

Vale destacar que no setor da saúde existem diversos procedimentos implementados que já atendem, direta ou indiretamente, a alguns dos direitos previstos na LGPD, como o da portabilidade. A portabilidade de plano de saúde implica necessariamente a transferência das informações do titular dos dados e prevê a proibição do preenchimento de novo formulário de declaração de saúde, com exceção dos casos em que o novo plano (plano de destino) tenha coberturas não previstas no plano de origem.

Além disso, o artigo 20 da Resolução nº 305 da ANS, que trata sobre o Padrão para a Troca de Informação de Saúde Suplementar (Padrão TISS), relacionado à troca de informações entre operadoras de planos de saúde e entre essas e seus prestadores, determina que é direito do titular obter das operadoras as informações de dados de atenção à saúde do Padrão TISS.

18. RESPONSABILIDADE PELO DESCUMPRIMENTO DA LEI

A LGPD traz uma série de sanções administrativas para o caso de descumprimento de seus preceitos (art. 52):

- Advertência com indicação de prazo para adoção de medidas corretivas;
- Multa simples de até 2% limitada a R$ 50 M (cinquenta milhões de reais) do faturamento da pessoa jurídica de direito privado por infração;
- Multa diária;
- Publicização da infração;
- Bloqueio dos dados pessoais a que se refere a infração até sua regularização;
- Eliminação dos dados pessoais a que se refere a infração;
- Suspensão do tratamento dos dados pessoais a que se refere a infração; e
- Proibição parcial ou total de exercer atividades de tratamento de dados.

Vale destacar que todas essas sanções são administrativas, ou seja, é possível que haja ainda eventual responsabilização por danos na esfera judicial.

19. RUMO À CONFORMIDADE!

A Lei Geral de Proteção de Dados impõe às empresas mudança de postura por parte de todos os seus integrantes. Para tanto, é necessário que se crie estrutura de governança em proteção de dados pessoais, com a distribuição de responsabilidades internas de controle para aqueles que farão a sustentação do programa de governança. Além disso, deverá haver treinamento dos colaboradores para que se mantenham sempre cientes e diligentes com as regras e procedimentos da organização. A eficácia de um programa de governança em proteção de dados pode ser inteiramente comprometida caso a cultura de privacidade da empresa não seja disseminada entre os colaboradores, que deverão estar comprometidos e alinhados com o cumprimento de todo o programa de privacidade da empresa.

A LGPD determina que Controladores e Operadores tenham registro de suas operações de tratamento de dados pessoais. Essa não é uma tarefa fácil, mas é um ponto de partida para que a empresa possa realizar um processo de autoconhecimento a respeito das suas atividades que envolvem o tratamento de dados pessoais. Assim, será necessário realizar o chamado *data mapping*, em que é necessário constar todo o ciclo de vida dos dados pessoais naquele processo, desde a sua origem, passando por eventuais compartilhamentos, transferência internacional, até o seu descarte.

Com esse mapeamento é possível verificar se há excessos no tratamento do dado pessoal, estabelecer com quais empresas há o compartilhamento de dados, identificar se as finalidades da atividade são eventualmente genéricas ou discriminatórias, adequar as bases legais e verificar quais operações podem implicar maiores riscos à empresa em razão das suas finalidades, contexto e dados envolvidos.

Feito isso e conhecendo todas as vulnerabilidades da empresa, é hora de criar a estrutura de governança que vai sustentar o programa de privacidade da empresa.

Para tanto, é importante que a empresa verifique qual será a sua estratégia em relação à privacidade, tendo em vista que o nível de maturidade poderá ser extremamente elevado (para além do necessário para atender às obrigações legais da LGPD) ou apenas o nível suficiente para estar em conformidade com a LGPD. No caso de empresas de saúde, pelo contexto de suas atividades, importante que se empenhem no processo de conformidade para além do necessário ao atendimento à LGPD, o que pode ser inclusive diferencial de mercado.

De todo modo, as empresas devem ao menos criar políticas de proteção de dados que deverão conter todos os pilares da governança a ser implementada na organização. Essas políticas precisam abranger todas as diretrizes a serem alcançadas por meio de procedimentos internos, como o de avaliação de terceiros, de resposta a incidentes, avaliação de riscos de novos projetos, manutenção do *data mapping*, classificação de dados pessoais, procedimento para expurgo seguro de dados pessoais, entre outros.

Avisos de privacidade também deverão ser criados com linguagem clara e acessível, como instrumento de transparência ao titular dos dados pessoais, para que esse possa se informar a respeito da operação de tratamento dos seus dados pessoais, além de reconhecer seus direitos. É prática bastante positiva criar avisos de privacidade para cada situação específica.

Com relação ao exercício dos direitos dos titulares, é necessário que a empresa crie mecanismos internos e canais próprios para garantir aos seus consumidores, terceiros e colaboradores o exercício dos seus direitos. A LGPD não traz fórmula pronta sobre como criar tal sistema de comunicação. Entretanto, solução plausível é o aproveitamento do SAC existente na empresa com um novo canal para que os titulares possam acessar e controlar seus dados.

A empresa deverá, ainda, se organizar para cumprir a obrigação legal de fornecer a confirmação de existência do tratamento ou o acesso a dados pessoais, de forma gratuita, simplificada e dentro do prazo legal de 15 (quinze) dias. Vale destacar que a solicitação depende da extensão da requisição, conforme previsto no artigo 19, incisos I e II, da LGPD. É preciso ressaltar ainda que esses prazos poderão sofrer eventual modulação em razão das particularidades dos setores regulados, como é o caso da Saúde, conforme artigo 19, §4º, da LGPD.

Outra questão que deverá ser considerada é a gestão dos terceiros com quem a empresa compartilhe dados pessoais. Nesses casos, deverá haver a adequação contratual para prever direitos, obrigações e responsabilidades, sempre observando a posição da empresa na relação, se Controladora ou Operadora.

Ao contrário do que ocorre no GDPR, que, em seu artigo 28, prevê as cláusulas mínimas a serem inseridas em um contrato, a LGPD foi silente nesse sentido. Entretanto, é razoável que haja cláusulas nas quais as partes se comprometam a garantir, por meio de medidas técnicas e administrativas, a depender do interesse das empresas envolvidas, o direito de uma auditar a outra periodicamente em relação à governança de dados pessoais.

Ainda, a recomendação é incluir as operações de tratamento de dados pessoais compreendidas na relação, suas finalidades, proibição de desvio da finalidade sem a autorização do controlador, responsabilidade por atender aos direitos dos titulares e por realizar notificações em caso de cocontroladores, possibilidade de subcontratação, regras específicas sobre a base de dados acessada ou construída durante a relação contratual, multas e direito de ressarcimento caso uma empresa sofra prejuízos em razão da falta contratual da outra entre outras cláusulas.

Além de todos os ajustes de normas, procedimentos e contratos já mencionados, é preciso que a empresa decida o quanto e como irá investir em tecnologia de segurança da informação, a fim de aprimorar suas estruturas tecnológicas com o objetivo de auxiliar a adequação à LGPD.

Partindo da premissa de que o programa de privacidade está criado com todas suas políticas e seus procedimentos, é hora de realizar treinamentos para os colaboradores. É boa prática que haja treinamentos gerais e específicos, tendo em vista que as áreas de uma empresa poderão ter atividades específicas com regras particulares, como a área de Recursos Humanos e a de Marketing. Além disso, para criar engajamento e sentimento de pertencimento, é recomendável que se criem eventos de privacidade para debater temas da atualidade, com materiais de identidade visual e de comunicação relacionados à proteção de dados pessoais.

A empresa ainda deverá indicar o *Data Protection Officer (DPO)* ou, nos termos adotados pela LGPD, o Encarregado pela Proteção de Dados Pessoais, que será um profissional ou uma pessoa jurídica responsável pela interface entre a empresa, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados.

Embora a LGPD não traga isso expressamente, é recomendável que a pessoa, física ou jurídica que exerça o cargo de DPO/Encarregado, tenha conhecimento jurídico e regulatório para que possa fazer a harmonização das normas da governança com as normas gerais de proteção de dados pessoais e as específicas eventualmente existentes no setor.

Conforme a LGPD, as funções típicas do DPO serão:

- aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- receber comunicações da Autoridade Nacional de Proteção de Dados e adotar providências;
- orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

A Autoridade Nacional de Proteção de Dados poderá, conforme artigo 41, §3º, criar outras funções para o Encarregado, além das já previstas na Lei e aquelas eventualmente atribuídas pela empresa que o contratou.

O Encarregado não terá responsabilidade pessoal em relação às multas eventualmente aplicadas pela ANPD, assim como não terá responsabilidade direta sobre indenizações devidas a titulares de dados pessoais. Contudo, caso o Encarregado concorra com culpa ou dolo no evento danoso ao titular do dado pessoal, a empresa poderá solicitar o ressarcimento dos prejuízos que teve, caso exista a possibilidade de direito de regresso.

O programa de governança em proteção de dados deve ser autossustentável, assim como revisado periodicamente para avaliação de sua eficiência. Ao analisar métricas como processos cujo risco fora avaliado em determinado período - número de riscos de privacidade que continuam pendentes após o período de mitigação, tempo de resposta após a notícia de incidentes de segurança, tempo de resposta às requisições dos titulares -, a organização procura estar sempre em conformidade, de maneira perene e persistente.

É importante que a empresa entenda que a privacidade de seus interlocutores, concretizada por meio da proteção de seus dados pessoais, é valor cuja busca é perene e jamais poderá retroceder ou afrouxar seus controles. Sendo assim, a mera implantação de controles e procedimentos internos é insuficiente, e sua reciclagem e atualização periódica são tarefas obrigatórias.

20. DIMINUINDO OS RISCOS DO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

É inegável que o tratamento do dado pessoal sensível acarreta risco maior. Assim, o agente de tratamento precisa criar métodos para diminuir os riscos no tratamento de dados, que é parte nuclear de qualquer negócio no setor da saúde.

Nesse cenário, conforme item 15 desta cartilha, é boa prática que todas as empresas, sobretudo aquelas que lidam com dados pessoais sensíveis de forma massiva, criem processos para avaliar projetos e produtos desde sua concepção sob a perspectiva da privacidade. É o chamado Privacy by Design, que requer a criação de uma metodologia para que proativamente seja inserido o cuidado com a privacidade desde a concepção de qualquer atividade relacionada à Tecnologia da Informação, Práticas de Negócio, Produtos, Infraestrutura de Rede etc.

A postura proativa da empresa em avaliar as suas operações com antecedência, assim como avaliar periodicamente a eficiência de seus controles, implicará a diminuição dos riscos no tratamento de dados pessoais.

21. CASOS DE VIOLAÇÃO DE DADOS PESSOAIS NA ÁREA DA SAÚDE

A violação de dados pessoais não se restringe somente à exfiltração de dados, mas abrange qualquer tipo de infração à LGPD. Em relação a incidentes de segurança, estará configurado sempre que houver perda de confidencialidade, de integridade ou disponibilidade.

A área da saúde já apresentou diversos casos de violação de dados pessoais no Brasil e no exterior. Com efeito, o GDPR, após o início de sua vigência em maio de 2018, teve sua primeira multa aplicada em razão de violação de dados pessoais ocorrida em hospital localizado em Portugal, cujo valor da multa foi de EU$ 400.000,00 (quatrocentos mil euros). Nesse caso, a Autoridade de Controle Portuguesa realizou investigação após denúncia lançada pela Ordem dos Médicos em junho de 2018.

A investigação verificou que havia 11 profissionais da área de serviços sociais com acesso a dados que deveriam ser acessíveis somente para médicos. Além disso, foi evidenciado que havia 985 contas ativas de médicos com acesso aos dados pessoais, sendo que somente 296 efetivamente trabalhavam no hospital. Por fim, restou evidenciado que o hospital não tinha regras claras sobre acesso aos dados pessoais, assim como para criação de perfis com acesso aos referidos dados pessoais de pacientes.

Na Holanda, outro hospital foi multado em junho de 2019 no valor de EU$ 460.000,00 (quatrocentos e sessenta mil euros) e houve a abertura de procedimento administrativo após a notícia de que 197 funcionários do hospital tiveram acesso a registros médicos de uma celebridade daquele país. No decorrer da investigação, a Autoridade Supervisora concluiu que o hospital não tomou medidas técnicas suficientes para evitar acessos indevidos, sobretudo no que concerne à dupla autenticação para acesso a sistemas que contenham o histórico médico dos pacientes. Assim, houve o entendimento de que o hospital falhou na sua obrigação, prevista no artigo 32 do GDPR, de garantir a confidencialidade dos dados que trafegam em sua estrutura, principalmente os de natureza sensível, sendo aplicada a multa pela Autoridade competente.

Não obstante a multa já aplicada, o referido hospital também se envolveu em outro incidente de segurança, referente ao vazamento de lista de transferência de pacientes, na qual constavam dados como nome, data de nascimento, enfermidades e remédios dos pacientes.

Por fim, é válido salientar que a LGPD destaca, principalmente no artigo 46 e seguintes, que o agente de tratamento é obrigado a adotar medidas técnicas e administrativas para garantir a segurança do dado pessoal, o que inclusive será considerado pela Autoridade Nacional de Proteção de Dados quando da análise de gravidade do incidente (art. 48, §3º, da LGPD).

No Brasil, podemos citar o caso de uma rede de drogarias que foi multada em quase 8 milhões de reais por condicionar descontos ao fornecimento do CPF do consumidor no ato da compra. Segundo a decisão proferida pelo PROCON/MG (Programa de Proteção e Defesa do Consumidor de Minas Gerais), órgão integrante do Ministério Público mineiro, a prática não somente viola o direito do consumidor em relação à informação clara e adequada sobre o serviço ofertado, como também por coletar dados pessoais dos consumidores sem que houvesse informação prévia.

22. GLOSSÁRIO

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

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

Encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;

ANPD: Autoridade Nacional de Proteção de Dados; e

LGPD: Lei Geral de Proteção de Dados.

CRÉDITOS

Sócios:

José Roberto Opice Blum

Renato Opice Blum

Marcos Bruno

Rony Vainzof

Caio Lima

Camilla Jimene

Danielle Serafino

Idealização:

Alessandra Borelli Vieira

Autoria:

Ana Maria Roncaglia

Diogo Marzzoco

Gabriela Silveira Bueno dos Santos

Coordenação editorial:

Lara Silbiger

Revisão:

Caio Lima

Diogo Luís Manganelli de Oliveira

Bruno Toranzo

Arte e diagramação:

Paola Cosentino

Lucas Fernandes