

A proteção de dados pessoais na área de saúde

Por Ana Paula Oriola De Raeffray (*)

Recentemente falei de maneira breve acerca dos efeitos da Lei Geral de Proteção de Dados Pessoais (“LGPD”) – Lei nº 13.709, de 14 de agosto de 2018 – na previdência complementar. Fiz um alerta, contudo, de que as entidades de previdência complementar que também são operadoras de saúde, terão que adotar medidas intensificadas na proteção dos dados dos participantes/usuários dos planos privados de assistência à saúde.

Na assistência à saúde, seja pública, seja privada, a amplitude das relações que são estabelecidas, entre as mais diversas partes, para a efetiva prestação dos serviços ao paciente é, sem exagero, imensa. Estão envolvidos, apenas para exemplificar, médicos, enfermeiros, hospitais, fornecedores de medicamentos e de equipamentos, laboratórios, operadoras de saúde, terapeutas. Todos os envolvidos acabam tratando dos dados pessoais dos pacientes.

A tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias é base legal para o tratamento de dados pessoais, conforme está previsto no artigo 7.º, inciso VIII, da LGPD. Entende-se por tratamento de dados, toda a operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

O dado pessoal referente à saúde, o dado genético e o dado biométrico são qualificados como sensíveis na LGPD podendo ser tratado, sem consentimento do titular apenas na hipótese em que for indispensável, na área de saúde, para a proteção da vida ou da incolumidade física do titular do dado ou de terceiro ou na tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.

Os diversos atores que participam da prestação de serviços de assistência à saúde inevitavelmente compartilham entre si os dados pessoais dos pacientes, mas na LGPD há restrição a este compartilhamento, pois está ali vedada a comunicação ou o uso compartilhado entre controladores desses dados sensíveis referentes à saúde com o objetivo de obter vantagem econômica, excetuando-se os casos de portabilidade dos dados, quando consentida pelo titular ou a necessidade de comunicação para a adequada prestação de serviços de saúde suplementar.

A vedação ao compartilhamento de dados com o fito de obter vantagem econômica é por si só uma restrição que sofrerá uma gama muito grande de interpretações e demandará regulamentação, pois a operadora de saúde, por exemplo, transmite os dados sensíveis para a sua rede credenciada de prestadores com objetivo econômico.

A própria exceção a essa vedação também passará por uma gama de interpretações, pois qual é a adequada prestação de serviços de saúde suplementar? Quais são as características dessa “adequada prestação.”

E o compartilhamento de dados entre os hospitais privados e a sua rede de prestadores, também se sustenta em objetivos econômicos, mas não foi indicada nenhuma exceção para estes casos na LGPD, o que faz pressupor, ao menos neste momento, que é vedado esse compartilhamento.

É claro que todas estas questões serão debatidas no processo de implantação da LGPD, que deverá ocorrer até agosto de 2020. Todos aqueles, todavia, que atuam na área de saúde terão que aderir à governança da segurança da informação, pois o tratamento de dados pessoais sensíveis, sem contar os dados pessoais de crianças e de adolescentes que também recebem tratamento diferenciado na LGPD, impõe maior responsabilidade, diante das expressas vedações legais.

O tratamento de dados sensíveis na área de saúde recebe regramento diferenciado em diversos países, observando-se regras rígidas para a segurança dos dados. Em 1997, diante do alargamento do National Health Service do Reino Unido, foram desenvolvidos os princípios para a segurança das informações e dados pessoais na área médica, estabelecidos no Relatório Caldicott, encomendado por Dame Fiona Caldicott, a National Data Guardian for

health no Reino Unido.

Os “Princípios Caldicott” são essenciais no desenho da governança da segurança da informação na área de saúde e, também, em todas as outras áreas que tratem dados sigilosos, haja vista que são extremamente objetivos. Em uma tradução livre, são os seguintes: 1) justifique o propósito para a utilização da informação confidencial; 2) não use o dado pessoal confidencial a não ser que seja absolutamente necessário; 3) utilize o dado pessoal confidencial o mínimo necessário; 4) o acesso ao dado pessoal confidencial deve ser restrito àquelas pessoas que necessitam conhecê-lo; 5) toda pessoa com acesso ao dado pessoal confidencial deve estar ciente de suas responsabilidades; 6) o acesso ao dado pessoal confidencial deve estar de acordo com a legislação; 7) a obrigação de compartilhamento do dado confidencial pode ser tão importante quanto a obrigação de proteger a confidencialidade dos dados do paciente.

A LGPD traz estes princípios na sua essência. Na área de saúde terá de ser desenvolvido um eficiente programa de governança, de compliance e de treinamento de pessoas para proteção dos dados sensíveis do paciente e a eficiência passa antes de mais nada pela conscientização das responsabilidades de cada um que participar da intrincada relação que se forma para a prestação da assistência à saúde.

(*) **Ana Paula Oriola De Raeffray** é Doutora em Direito pela Pontifícia Universidade Católica de São Paulo (PUC/SP). Professora dos cursos de pós-graduação da PUC/SP, sócia da Raeffray Brugioni Advogados, diretora vice-presidente do Instituto Brasileiro de Previdência Complementar e Saúde Suplementar (Ipcom).

Fonte: [Fausto Macedo – O Estado de S. Paulo](#) , em 20.04.2019.