



A nova Lei Geral de Proteção de Dados (LGPD) deve impor grandes mudanças ao setor de saúde suplementar ao ter que garantir o sigilo, não apenas médico, mas, também, de contato dos clientes. Nesta entrevista, a especialista Lidiane Mazzone apresenta os desafios e as situações que devem nortear os profissionais que atuam no mercado.

Lidiane é professora da Conhecer Seguros, advogada especialista em Direito da Saúde e Regulação da Saúde Suplementar, e mestre em Saúde Coletiva, pela Faculdade de Medicina da USP. Ela também ministra o curso online “Lei Geral de Proteção de Dados e as Operadoras de Planos de Saúde”, indicado a todos os profissionais ligados à saúde, em especial as operadoras e os corretores de seguros.

Conhecer Seguros: A LGPD é um tema relativamente novo e já tem causado muitas dúvidas. Para quem atua no setor de saúde suplementar, quais os principais desafios para aplicação da lei e seus impactos diretos?

Lidiane Mazzone: O principal desafio para quem atua com saúde suplementar é a mudança de cultura que a LGPD vai impor ao mercado. Hoje, o mercado de saúde se preocupa com a proteção do sigilo médico. No entanto, a proteção dos dados pessoais do titular envolve outras preocupações, como a prestação de informações ao titular e condutas como tratamento mínimo. A maioria dos agentes desse mercado tem a consciência da proteção dos dados e o tratamento acaba, muitas vezes, por desconsiderar a vontade do titular. Com a nova lei, isso terá que mudar.

CS: No caso das operadoras de planos de saúde, que manipulam informações sensíveis dos beneficiários, quais as medidas de segurança dos dados que devem estabelecer?

LM: As operadoras de planos de saúde devem primeiramente conscientizar os times sobre a importância da implementação do programa de proteção de dados, para que não seja encarado como uma obrigação ou uma auditoria. Em seguida, entendo que o mapeamento dos dados é o mais importante para identificar as inconsistências que poderão gerar problemas e prejuízos no decorrer da operação. Identificados os pontos mais críticos, fica mais fácil desenhar um programa de ação para solucionar as questões que mais demandarão atenção das operadoras.

CS: Sabemos que quem repassa essas informações às operadoras são os corretores de

seguros. Em um eventual vazamento ou uso inadequado dos dados, eles podem ser responsabilizados? Quais cuidados devem tomar?

LM: Dentro da cadeia de tratamento de dados, onde esses dados pessoais são transferidos entre os atores do mercado, a responsabilidade é solidária perante o titular. Em outras palavras, todos deverão ter o mesmo cuidado com os dados pessoais, porque respondem igualmente perante o beneficiário. No entanto, é preciso que os instrumentos contratuais entre tais agentes contenham as previsões sobre a responsabilidade nessa cadeia, bem como quais as providências são exigidas como mínimas para compreensão que o dever de cuidado foi tomado. Caso violado esse pacto, a parte prejudicada poderá buscar reparação contra a parte que causou o prejuízo.

CS: Existem estatísticas a respeito do uso inadequado de dados no setor de saúde suplementar no Brasil ou no mundo?

LM: O estudo mais interessante neste caso é o da IBM, no "Relatório sobre o prejuízo de um vazamento de dados 2020". No relatório, o setor de saúde é indicado como o que mais sofre prejuízos no mundo com o vazamento de dados. Pelo décimo ano consecutivo, o setor de saúde teve o maior prejuízo médio de um vazamento, com US\$ 7,13 milhões, um aumento de 10,5% em relação ao estudo de 2019. Os setores de saúde, energia, financeiro e farmacêutico tiveram um prejuízo total médio de um vazamento de dados significativamente mais alto do que os menos regulamentados. O relatório informa ainda que o setor de saúde teve o tempo médio mais alto para identificar e conter um vazamento, com 329 dias, enquanto o financeiro teve o menor tempo médio, com 233 dias.

CS: O vazamento, por ações de hackers por exemplo, pode prejudicar também a reputação da operadora. Qual a força da boa reputação no quesito segurança dessas empresas?

LM: A reputação é o ponto principal de confiabilidade dos consumidores do serviço e por certo passará a ser um grande ativo. O legislador tem em mente que algumas das penalidades aplicadas aos agentes infratores não é somente a multa, mas, sim, a exigência de publicidade do vazamento, medida que afeta diretamente a reputação da empresa. Com a reputação abalada, os consumidores poderão trocar de operadora, buscando aquela que apresenta a melhor forma de tratamento de dados de forma segura. E essa preocupação já passou a ser latente, o que se nota pelas notícias de vazamento que a cada dia mais causam espanto no público em geral.

CS: As operadoras e os corretores não apenas têm acesso a dados sensíveis, como contato e documentos, mas também informações sigilosas sobre o estado de saúde dos pacientes. Essas informações devem ser compartilhadas de modo constante com o SUS pela internet. Quais cuidados devem ser reforçados nessa transação para que o conteúdo não caia em mãos erradas?

LM: Os cuidados das operadoras de planos de saúde na transmissão de dados para o SUS deverá ser refletido no emprego das melhores técnicas para a preservação e para a segurança. Por isso, é importante que os sistemas de segurança estejam alinhados com as necessidades da operadora, para que possam garantir que as melhores técnicas sejam empregadas nas atividades. Aqui, o mapeamento dos dados bem elaborado também é um diferencial, pois através dele a empresa consegue identificar suas fragilidades e quais as medidas tomadas para sanar tais "gaps" na operação.

CS: Diante de todo esse cenário, aumentou a procura pelo seguro de cyber risks para garantir maior segurança? O que pode ser feito para aumentar as vendas deste produto?

LM: O seguro de cyber risk é um excelente produto para minimizar eventuais riscos das operadoras de planos de saúde. Acredito que com o avanço dos projetos de implementação da LGPD pelas empresas, a opção pelo seguro será vista como um atrativo para os riscos mais vulneráveis que

elas estão expostas. O conhecimento sobre conceitos principais e penalidades previstas pela legislação também poderá auxiliar no crescimento desse tipo de seguro.

CS: Você ministra as aulas do curso "Lei Geral de Proteção de Dados e as Operadoras de Planos de Saúde" da Conhecer Seguros. Qual a necessidade do treinamento para o corretor e quais situações o curso aborda?

LM: O treinamento para os corretores é essencial. Primeiro, por serem um importante elo da cadeia de tratamento de dados dos beneficiários, devendo estar cientes de sua responsabilidade e seus riscos diante das regras da LGPD. Segundo, pela própria oportunidade de comercialização de seguro de cyber risks para as empresas, eis que a LGPD se aplica para todo o mercado e todos os agentes deverão tomar as medidas necessárias para o controle dos riscos. O curso aborda os conceitos principais aplicados pela lei, bem como analisa as operações do mercado de planos de saúde, trazendo alertas sobre as melhores condutas a serem tomadas. O curso também traz casos interessantes que podem auxiliar na compreensão de melhores práticas para o setor.

Para saber mais e se inscrever no curso “Lei Geral de Proteção de Dados e as Operadoras de Planos de Saúde”, [clique aqui](#).

Fonte: Conhecer Seguros, em 19.02.2021