Por Carlos Alberto Ferraiuolo Jr (*)

No Brasil, temos dois grandes desafios que exigem das organizações de saúde a implementação de um eficiente sistema de governança da informação: a LGPD (Lei Geral de Proteção de Dados), prevista para entrar em vigor em agosto de 2020, que estabelece regras sobre a coleta, o tratamento, o armazenamento e o compartilhamento de dados pessoais gerenciados pelas organizações; e a Lei do Prontuário Eletrônico, que dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente, publicada em dezembro de 2018.

A má notícia para os responsáveis pelas políticas de governança da informação é que registros médicos são um dos alvos preferidos dos hackers. E violações e uso indevido de dados podem levar a roubo de identidade e processos caros.

Quando pensamos no ciclo de vida dos dados pessoais sensíveis na saúde, devemos lembrar que há todo um ecossistema interligado, que vai da clínica médica ao hospital, passa pelo laboratório, a farmácia, o próprio paciente e os agentes de saúde, bem como toda a esfera pública – como o Sistema Único de Saúde (SUS). Ou seja, alcança desde o registro de um simples cadastro em um consultório até a entrada em um Pronto Socorro de um hospital (público ou privado) e os dados ficam armazenados em cada uma dessas etapas.

Por isso, é preciso controlar quem tem acesso a esses dados confidenciais, com sistemas de gestão documental que integrem senhas e regras de permissão que garantam que as políticas de governança da informação sejam observadas em todo o seu ciclo de vida. O objetivo é que ferramentas integradas permitam estar sempre à frente dos requisitos de conformidade, o que significa que os documentos estejam sempre prontos para auditorias.

O treinamento deve ser um esforço contínuo para educar funcionários sobre políticas, ameaças atuais e como lidar com elas. E como os colaboradores são citados como o elo mais fraco na segurança digital, devem ser tratados como qualquer outro ponto de vulnerabilidade na empresa, com instruções claras sobre as ameaças de segurança que podem vir a enfrentar, e também, as consequências caso não sigam as práticas de um sistema eficiente de governança da informação. Na verdade, tudo é uma questão de alinhar pessoas, processos e tecnologia para a implementação de soluções de gestão documental que garantam a segurança digital das informações em todo o seu ciclo de vida, com customização e aplicação de regras de conformidade e de temporalidade.

Para fugir das multas e sanções previstas pela LGPD, todo cuidado é pouco.

(*) **Carlos Alberto Ferraiuolo Jr.** é diretor de tecnologia e produtos da Access.

Fonte: Saúde Business, em 07.01.2020