Por Marcos Tadeu (*)

A segurança da informação nunca foi tão amplamente debatida como atualmente. Em grande evidência desde a aprovação da Lei Geral de Proteção de Dados (LGPD), no ano passado, o tema é preocupação constante de empresas dos mais diferentes segmentos. Alguns setores específicos, como o financeiro e o de saúde, já convivem com regulamentações relacionadas à proteção de dados pessoais há algum tempo, porém, agora, as restrições se intensificaram.

No que se refere às organizações do segmento de saúde em geral e de hospitais especificamente, o tema é ainda mais delicado, uma vez que a LGPD classifica no Art, 5º os dados referentes à saúde, dados biométricos e dados genéticos na categoria de dados sensíveis. Os dados sensíveis são objeto de tratativa diferenciada na LGPD, existindo toda uma seção específica a respeito dos mesmos na Lei.

Evidentemente a coleta, armazenamento, processamento e a tratativa de dados pessoais de saúde fazem parte das atividades de uma organização desse segmento. Sendo as mesmas informações essenciais para profissionais e empresas relacionadas poderem prestar os serviços e atendimento relacionados à sua atividade fim. Por exemplo: diagnóstico de doenças, acompanhamento da saúde dos pacientes, histórico de exames, entre outros. Essa legitimidade para manejar dados pessoais sensíveis das organizações do setor de saúde implicam na responsabilidade de tratá-los de acordo com os preceitos da LGPD, ou seja, protegê-los e estar prontos para dar respostas a demandas embasadas nessa Lei.

Um estudo realizado pelo Serasa Experian, em junho deste ano, sobre como as empresas brasileiras estão se preparando para atender às exigências da LGPD apontou que o setor de saúde e hospitalar está em último lugar entre os segmentos analisados. Somente 8,7% das instituições estão totalmente preparadas. É necessário agilizar esse processo!

Entre as obrigações a serem cumpridas estão designar o “Encarregado” (conhecido no mercado como Data Protection Officer – DPO), identificar onde as informações pessoais estão armazenadas (Classificação da Informação) e implementar controles e processos condizentes para garantir e demonstrar a segurança.

A LGPD não faz distinção entre dados em ambientes tradicionais de TI (conhecidos no mercado como on premisses) e ambientes de TI em nuvem (Cloud). Se os dados são coletados por uma organização, mesmo que os mesmos sejam processados ou armazenados por uma outra organização, a entidade que coletou os mesmos é responsável por esses dados pessoais.

É importante destacar que o modelo de segurança de provedores de nuvem pública é um modelo de segurança compartilhada, onde cabe ao cliente final a responsabilidade de implementar os controles e configurações de segurança necessários utilizando as tecnologias disponíveis. O provedor de nuvem disponibiliza algumas tecnologias de segurança (VPN, criptografia, Firewall, Autenticação, etc) mas cabe ao cliente configurá-las e utilizá-las adequadamente, assim como desenvolver e implementar os processos de negócio de forma segura, como também processos de controle de segurança.

A tecnologia de nuvem é parte essencial da transformação digital pela qual as organizações estão passando. No segmento de saúde isso é ainda mais evidente, pois a eficiência de um hospital engloba o compartilhamento de informações entre diferentes setores – médicos, enfermeiros, farmacêuticos e, até mesmo, a área administrativa – e a nuvem pode ser parte essencial desse processo.

A adoção do prontuário eletrônico, por exemplo, melhora a experiência do paciente e a segurança do tratamento. A unificação dos dados da tecnologia com os de farmácia, agiliza a separação dos medicamentos prescritos pelo médico e possibilita, posteriormente, a conferência da dosagem pelo

enfermeiro no leito. Porém, para que o resultado seja efetivo, é necessário coletar dados dos pacientes, armazená-los e manuseá-los. Além disso, precisa haver integração com outros departamentos.

Contar com tecnologias de armazenamento em nuvem simplifica esse processo, pois os dados podem ser acessados de qualquer ambiente com base em regras pré-determinadas. No entanto, o simples fato de implementá-las não garante a segurança e privacidade das informações. É preciso continuar a investir em soluções de segurança, proteção e controle para evitar que alterações acidentais, compartilhamentos indevidos e invasões do sistema aconteçam. Atualização, manutenção e otimização constante dos sistemas de segurança, aliado ao treinamento de funcionários, garante um ecossistema mais seguro e eficiente.

Para que o setor da saúde se adeque totalmente e esteja preparado para as novas demandas de segurança da informação, são necessários ajustes nos procedimentos, profundo conhecimento das informações que estão sendo armazenadas, quer seja em ambiente próprio ou nuvem, assim como investimentos em tecnologia e infraestrutura. Certificar que os dados, internos e dos pacientes, estão armazenados de forma segura é o primeiro passo para a prestação de um serviço mais transparente e eficaz – e em conformidade com as regras de privacidade.

(*) **Marcos Tadeu** é gerente de engenharia de sistemas da Veritas Brasil.

Fonte: Saúde Business, em 03.12.2019