Por Gabriel Couto (*)

Desde a aprovação da Lei Geral de Proteção de Dados (LGPD) em 2018, formou-se um enorme frenesi em torno da segurança digital. Empresas e os cidadãos começaram a preocupar-se mais com o uso de dados e a maneira com que eles são compartilhados, armazenados e protegidos. No ecossistema da saúde não poderia ser diferente. Isso ficou ainda mais evidente, após a portaria do Ministério da Saúde que autoriza e regulamenta o exercício de telemedicina no Brasil, durante a pandemia de Covid-19. Neste contexto, ganham relevância ainda maior os aspectos relacionados às práticas de proteção aos dados das plataformas que prestam esse tipo de serviço e de outras que viabilizam as demais etapas dos processos, como é o caso da emissão da receita médica digital. A pergunta clássica é: será que os meus dados estão realmente seguros?

Para começarmos essa conversa, é importante salientar que é proibido por lei a quebra do sigilo médico, ou seja: os dados dos pacientes são privativos e só podem ser acessados por ele, por seu médico e por pessoas com as quais o paciente opte por compartilhá-los. Apesar de haverem algumas exceções judiciais que permitam essa quebra de sigilo, o código de ética é levado a sério, desde sempre, pelos profissionais da saúde, que conhecem bem as consequências de suas ações nesse sentido. Obviamente, essa preocupação acaba transferindo-se para desenvolvedores das tecnologias usadas, seja na gestão dos hospitais e clínicas, ou no atendimento clínico, o que incluem as plataformas de telemedicina, prontuários eletrônicos e as que geram a receita médica digital.

Convém somente fazer um parêntese antes. Quando falamos de receita médica digital não estamos falando de tirar uma foto de uma receita manuscrita, enviada via whataspp ou qualquer outro meio digital, e apresentá-la no balcão da farmácia. Estamos falando de uma plataforma, especialmente criada com essa finalidade, que tem por detrás do seu desenvolvimento aspectos que visam garantir tanto a segurança do paciente, do ponto de vista de sua saúde, e como da privacidade de dados. Usando a tecnologia, no momento da prescrição, o médico poder contar com recursos de apoio como uma base de dados de medicamentos e exames, que aliada às ferramentas de apoio à decisão clínica, auxilia os médicos a tomar suas decisões. É possível saber quando um medicamento interage com outro, por exemplo, ou até quando o paciente tem alergia a algum princípio ativo do medicamento receitado – tudo em tempo real.

Falando especificamente da segurança digital, políticas de segurança de dados ajudam a garantir a privacidade. Aqui, gostaria de dar o exemplo de como isto acontece com a plataforma de prescrição que desenvolvemos, desde 2012. Termos de confidencialidade são assinados pelos colaboradores; o acesso ao banco de dados é restrito a membros da camada diretiva de tecnologia e, além de requerer duas camadas de autenticação, a conexão é criptografada. No caso das informações relacionadas às prescrições, como medicamento e nome do paciente, o acesso é ainda mais controlado, todas as ações ficam salvas para posterior auditoria e para garantir que as leis do país sejam seguidas, todos os dados da plataforma são hospedados no Brasil. Para os dados que precisam ser mantidos, um mapa traz informações sobre o motivo para que cada um deles seja preservado, o tempo que ficará armazenado e também a lei que determina essa ação. Mesmo os relatórios que são acessados por toda empresa têm regras aplicadas, os dados são estatísticos e nunca possuem identificadores pessoais (nome, documentos, endereço, entre outros).

Além disso, para evitar o risco de vazamento nos ambientes de desenvolvimento e de teste, não são utilizados dados reais. O time de desenvolvedores conta com apoio de um software que gera dados fictícios; e nenhum script de terceiros, como por exemplo, do Google Analytics, é empregado nas áreas da plataforma que possuem dados sensíveis. Sem dúvida, essas questões todas chegam até a dificultar o desenvolvimento, mas é algo que não podemos abrir mão. É preciso sempre tomar uma série de cuidados e isso inclui a integração com terceiros. No caso de nossa plataforma ser incorporada em outras soluções, como de prontuário eletrônico, o parceiro só tem acesso às prescrições feitas através do seu software.

É muito comum as pessoas se sentirem seguras quando falamos que os “dados são criptografados”, mas a maior parte das falhas de segurança encontradas em histórias de grandes vazamentos de dados está relacionada a falta de conscientização e mapeamento de processos. Por isso, juntamente com uma consultoria, fizemos uma série de entrevistas com todos os nossos colaboradores, mapeando cada processo e cada dado utilizado, conscientizando cada colaborador sobre sua responsabilidade, sobre o que é coletar/processar/tratar/armazenar um dado, e sobre as boas práticas de segurança.

Empresas sérias e comprometidas com a ética, mais do que estarem 100% em conformidade com a Lei Geral de Proteção de dados, têm como ponto focal o seu propósito: promover a digitalização da saúde, criar um ecossistema digital e, o mais importante, ajudar a salvar vidas. E, é fácil identificá-las não só pelos aspectos técnicos mencionados acima, mas também observando outras questões que podem ser perceptíveis aos mais leigos, como o histórico, ou os termos de compromisso de contrato que garantem que quaisquer dados cedidos pelos usuários não serão compartilhados e nem comercializados. Sem dúvida a tecnologia está aí mais disponível e útil do que nunca. Devemos tirar proveito dos seus benefícios e vantagens que elas podem trazer para a vida e a saúde de todos, em especial em momentos tão sensíveis e críticos, como esse que estamos vivendo com a pandemia causada pela Covid-19.

(*) **Gabriel Couto** é CTO da Memed.

Fonte: Medicina S/A, em 08.06.2020