Segurança da informação no SUS.
Dados de Saúde: A Corrente que Protege a Vida

Antigamente, o tratamento de dados pessoais era predominantemente analógico. Atualmente, com a modernização das clínicas e hospitais, aliada à adoção de plataformas integradas de saúde digital, esse processamento tornou-se majoritariamente eletrônico.
No entanto, o "prontuário na nuvem" traz uma responsabilidade que transcende a esfera clínica: a Segurança da Informação (SI). É imperativo compreender que o vazamento de um dado de saúde não representa apenas uma falha administrativa; trata-se de uma violação da dignidade humana e um obstáculo ao livre desenvolvimento da personalidade.

O Conceito de Dado Sensível na LGPD

A lei 13.709/2018 no artigo 5º, inciso II, tratou com rigor especial sobre o que considera sensível o dado que retrata *sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à* ***saúde*** *ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.* Aqui em saúde, abrange-se a mental e física.

Dados médicos são "sensíveis" porque revelam a intimidade mais profunda do indivíduo (doenças, histórico genético, orientações sexuais). O impacto de um vazamento nesse caso é irreversível, porque não se "troca" um histórico médico como se troca uma senha de banco.

A Segurança como uma Cadeia contínua de atitudes

Para aumentar a eficiência nas ferramentas de proteção de dados, o governo federal tem estimulado as boas práticas através de seminários como a 3ª Jornada de Proteção de Dados Pessoais no SUS realizadas dias 10 e 11/02/2026 com o objetivo de consolidar o compromisso do Sistema de Saúde com a proteção de dados pessoais, a privacidade do cidadão e a aplicação efetiva da LGPD no setor da saúde.

Para reforçar a conscientização sobre proteção de dados, governança e segurança da informação no setor de saúde, no último dia 11 deste mês, a Secretaria de Informação e Saúde Digital do Ministério da Saúde (SEIDIGI/MS), em parceria com a Secretaria de Segurança da Informação e Cibernética do GSI/PR promoveram o seminário de segurança da informação na saúde com o objetivo de dialogar sobre boas práticas e o fortalecimento da cultura de segurança da informação no Sistema

Único de Saúde (SUS), em um contexto de expansão da saúde digital e do uso de dados no cuidado e na gestão em saúde.

Esse intercâmbio entre instituições reforça que proteger dados é cuidar da integridade das vidas dos pacientes.

Nesse sentido, a segurança não é um "produto" que se compra, mas uma cultura na mudança de postura.
Temos uma relação que se completa através do elo tecnológico e do elo humano, onde os sistemas criptografados e firewalls são tidos como nível básico para a segurança tecnológica. Quanto ao elo humano, é crítico, visto que de nada serve o melhor sistema se a senha está no post-it pendurado no balcão ou o acesso é compartilhado entre turnos.

É possível afirmar que a segurança da informação na saúde pode chegar a uns 20% (vinte) quanto a tecnologia e 80% (oitenta) no que tange ao comportamento das pessoas.

Responsabilidade Compartilhada: De quem é a culpa?

Na cadeia de atitudes, todos se responsabilizam na medida de suas atribuições, pois cada clique no sistema reflete em uma vida na ponta do processo, por exemplo, a instituição deve investir em governança e treinamento de seus colaboradores, devendo fornecer as ferramentas, firewalls, backups e controle de acesso a quem pode ver.

No tocante ao profissional de saúde, este tem o dever ético e jurídico de preservar o sigilo médico no âmbito digital, com a adoção de protocolos de logout, não compartilhamento de senhas e cautela ao acessar dados em dispositivos móveis, pois deve evitar o "vazamento" de fotos ou diagnósticos.

Um dado se tornar inacessível ou corrompido em uma emergência, fica tão perigoso quanto um erro médico.

O paciente também possui o papel de zelar por seus dados de acesso aos portais de resultados de exames.

O ponto crítico deve-se voltar ao recepcionista porque é ele a porta de entrada e, muitas vezes, a vulnerabilidade.

Consequências Além da Multa

Além das sanções previstas nas resoluções da Agência (ANPD), o prejuízo mais severo é a **erosão da confiança no sistema de saúde**. As redes de confiança são

fundamentais para o sucesso de qualquer empreendimento de saúde, sendo que um incidente de segurança pode ser fatal para a reputação da clínica ou hospital.

Ética e Tecnologia Caminham Juntas

Não existe tecnologia que salve uma instituição sem cultura. A arquitetura humana é o desenho de como as pessoas se organizam, quem toma as decisões e como a ética digital é vivida no corredor do hospital. É o amadurecimento de entender que o dado pertence ao paciente, e nós somos seus guardiões.

Por isso, na era digital, o sigilo médico não é mais apenas uma questão ética de consultório, mas uma infraestrutura crítica de cidadania.

Se o dado não flui com segurança, o atendimento para e vidas são atingidas. Portanto, proteger o dado pessoal é, em última análise, proteger a integridade física e mental do paciente. Deve-se ter organização, pois o cuidado médico começa antes mesmo da consulta: começa no zelo pela privacidade de quem confia sua vida ao sistema.