Lista 1 - Sigilo garantido?

Rayane Cordeiro Barbosa

• As possíveis vulnerabilidades na confidencialidade, integridade e disponibilidade das informações médicas são:

→ Confidencialidade: acesso não autorizado (funcionários podem acessar informações de pacientes sem permissão); interceptação de dados em trânsito (durante a transmissão ao utilizar conexões inseguras por exemplo); vazamento de dados (perda ou roubo de dispositivos que contêm informações de pacientes).

→ Integridade: alteração de dados por pessoas não autorizadas e inserção de dados falsos no sistema, podendo levar a decisões equivocadas.

→ Disponibilidade: perda de dados devido a falhas em sistemas de armazenamento ou backups inadequados e acesso a dados indisponíveis por conta de falhas no sistema

• Riscos para pacientes e médicos:

→ Pacientes: exposição de informações pessoais sensíveis (violação da privacidade); prejuízo a reputação (divulgação de informações confidenciais); tratamentos inadequados caso haja alguma adulteração das informações médicas e chantagem.

→ Médicos: responsabilização por danos causados em decorrência de vazamentos de informações; perda de credibilidade e sanções éticas decorrentes da má gestão de informações sensíveis dos pacientes.

• Uma boa política de segurança deve contemplar os seguintes aspectos: criptografia, controle de acesso, backup regular, treinamento dos profissionais sobre como tratar as informações dos pacientes, utilização de firewalls, antivírus e sistemas de detecção de intrusão, plano de contingência para lidar com incidentes de segurança, conformidade com a legislação sobre a proteção de dados, auditoria regular para verificar vulnerabilidades e conformidade com as políticas de segurança além da gestão de riscos.