Telemedicina segura: compliance e proteção da informação

Por Carlos Souza (*)

A telemedicina ganhou impulso com o cenário apresentado em 2020, avançando em termos de oferta e tecnologia. Em virtude desta evolução, torna-se adequado pensar em elevação de maturidade e segurança da informação, sobretudo em termos de compliance regulatório e proteção da informação.

A criação, a implantação e o monitoramento contínuo de um programa de compliance devem ser considerados como parte integrante de um framework sólido e que tenha pontos de conexão com temáticas já existentes, tal como a adequação de diretrizes e políticas, ou até mesmo a criação destas, que é um elemento fundamental para o desdobramento das operações de maneira estruturada, o que não é uma tarefa fácil.

Tais desdobramentos devem resultar em uma operação padronizada e sustentada por meio de procedimentos gerenciais, operacionais e com instruções de trabalho aplicáveis, que devem ser elaborados de acordo com o grau de criticidade identificado. Certamente, processos

estabelecidos requerem ações de capacitação para que os atores de cada atividade garantam a qualidade percebida e a geração de valor para o paciente beneficiado pelo uso da telemedicina.

A capacitação contínua, traduzida em um plano efetivo de treinamento baseado em aprimoramento e solução de gaps, permitirá que a instituição seja beneficiada pela ação de profissionais que dominem e performem suas ações com excelência.

Já a auditoria interna apresentará um papel fundamental no atendimento ao vasto cenário regulatório federal, estadual e municipal, de órgãos de classe, assim como de certificação e de acreditação. É desejado que o olhar de conformidade identifique pontos em comum que sejam tratados de maneira diferente, embora complementares em cada temática.

Igualmente importante é o assunto relacionado à proteção da informação, especialmente no que se refere ao tratamento de dados pessoais e dados pessoais sensíveis, ambos presentes em toda jornada do paciente no uso da telemedicina.

A minimização da coleta de dados deve ser um agente de mudança. O mapeamento, a identificação e o uso apenas dos dados necessários reduzem a exposição ao risco e seus impactos em caso de incidentes. A exemplo do que ocorre na LGPD (Lei Geral de Proteção de Dados), a gestão de consentimentos e atendimento às solicitações de dados depende de um completo e correto entendimento do fluxo de informações nos processos envolvidos, o que vale também para o compartilhamento de dados com terceiros.

A segurança de informação deve apresentar foco na prevenção ao vazamento de dados, ao monitoramento de incidentes e à gestão das atualizações de segurança, o que evita estar vulnerável à aplicação de sanções que possam afetar a saúde financeira e a reputação da instituição.

O monitoramento de incidentes, em todos os ambientes, atenderá ao requisito básico por meio do qual só é possível tratar o que conhecemos e medimos. Agilidade, acuracidade e entendimento da abrangência do incidente são elementos essenciais para elaboração e execução de plano de resposta.

Todos estes elementos reunidos devem ser o motor de aprimoramento dos serviços de telemedicina, independentemente da natureza ao atendimento. Desdobrar os aspectos citados permitirá uma visão clara sobre oportunidades e fragilidades, resultando em um planejamento efetivo para alavancar a maturidade da prestação de serviços e consolidação do reconhecimento de que a telemedicina é segura.

(*) **Carlos Souza** é gerente de riscos e performance na ICTS Protiviti, empresa especializada em soluções para gestão de riscos, compliance, auditoria interna, investigação, proteção e privacidade de dados.

Fonte: Portal Hospitais Brasil, em 18.01.2021