Por André Cilurzo, Jefferson Kiyohara e Rodrigo Castro

Em fevereiro de 2026, o Conselho Federal de Medicina publicou a Resolução CFM nº 2.454/2026, documento que normatiza o uso da inteligência artificial (IA) na medicina. Sob a ótica dos negócios, significa novas exigências regulatórias e novas fontes de riscos para hospitais, empresas de medicina diagnóstica e clínicas. E isto traz impactos para os profissionais de Gestão de riscos, Compliance, Segurança de Informações, Privacidade e Auditoria Interna das organizações de saúde. E vale destacar que o impacto no ecossistema é amplo, por exemplo, alcança as seguradoras que operam no ramo saúde, ou vida com cobertura por invalidez, mesmo não sendo o público-alvo direto da norma, que passa a ser uma referência de boas práticas e uma expectativa crescente de reguladores, auditores e clientes corporativos.

O primeiro ponto importante da nova resolução do CFM, citado nos artigos 1º e 9º, é a necessidade de que modelos, sistemas e aplicações sejam auditáveis ou monitoráveis. Nesse contexto, já existe hoje um conjunto consistente de soluções de monitoramento e auditoria tanto para os LLMs abertos ao público quanto para as aplicações corporativas desenvolvidas pelas próprias instituições de saúde. No primeiro caso, agentes nos endpoints e extensões de navegador registram todas as interações dos profissionais com os modelos públicos, e permitem o monitoramento contínuo do uso e aplicam, em tempo real, políticas de uso previamente definidas pela instituição, de forma a assegurar o cumprimento estrito das diretrizes do CFM quanto à rastreabilidade, accountability e aderência a normas internas e externas.

No segundo caso, nas aplicações proprietárias de IA generativa utilizadas em fluxos assistenciais, os chamados firewalls de IA se posicionam tecnicamente entre o médico e a aplicação de IA, atuam como camada de controle e governança, aplicam regras e políticas aprovadas pelos comitês internos, registram e armazenam todas as interações realizadas e implementam *guardrails* técnicos e operacionais para evitar usos inadequados, mitigar vieses e reduzir o risco de respostas potencialmente danosas. Dessa forma, a organização passa a demonstrar, de forma documentada e auditável, que monitora o uso da IA, aplica controles preventivos e mantém trilhas de auditoria aptas a subsidiar as áreas de Gestão de riscos, Compliance, Segurança da Informação, Privacidade e Auditoria Interna no atendimento às novas exigências trazidas pela Resolução

Já nos artigos 5º e 11o, é garantido ao paciente, o direito de ser informado, de forma clara e acessível, quando modelos, sistemas e aplicações de IA forem utilizados como apoio relevante em seu cuidado, diagnóstico ou tratamento. Isto requer um inventário estruturado e atualizado do uso de IA e agentes de IA, e uma comunicação simples, objetiva e efetiva.

Já no artigo 6º, é reforçado o papel do médico diante da Lei Geral de Proteção de dados Pessoais (LGPD), no sentido de zelar pela confidencialidade, integridade e segurança dos dados de saúde do paciente. Tópico complementado pelos artigos 16º e 17º. Além do treinamento e orientações sobre o tema para os médicos, é fundamental ter políticas claras, processos e ferramentas que apoiem o cumprimento destas regras, além do devido enquadramento às bases legais definidas nos artigos 7º e 11º pela LGPD.

As soluções de tecnologia existentes também permitem a aplicação de regras para anonimização de informações sensíveis e confidenciais, bloqueando o envio delas às ferramentas de IA. Com essa prática, a empresa assegura uma proteção adicional, pois os dados deixam de ser tipificados como pessoais, eliminando o risco de eventuais penalidades pela LGPD em caso de vazamento de informações. Vale ressaltar a boa prática de descarte de dados, quando possível, visto que dados de prontuários médico eletrônicos dispensam prazo de retenção exigido pela LGPD. Essa prática reduz a exposição da instituição médica a incidentes de dados e vazamento de informações.

O uso de IA também traz novos desafios no âmbito da publicidade médica, tópico sempre relevante sob a ótica do compliance regulatório da saúde. Este tópico é coberto no artigo 7º, § 3° da resolução. Vale também lembrar dos requisitos da LGPD, exigindo que qualquer publicidade não

exponha dados de pacientes, visto que dados médicos são caracterizados como Dados Pessoais Sensíveis (todo e qualquer tipo de dado que possa causar discriminação ao titular de dados).

Outro ponto muito relevante para profissionais GRC está no artigo 14º, que "*a instituição médica ou o médico que desenvolver ou contratar um modelo, sistema e/ou aplicações de IA deverá estabelecer processos internos de governança aptos a garantir a segurança, a qualidade e a ética*". E no caso de instituições de saúde que adotem sistemas próprios de IA, é necessária a criação de uma comissão de IA e Telemedicina, subordinada à Diretoria Técnica. Tendo em vista que tais instituições também tratam dados pessoais de maneira massiva, o envolvimento do Encarregado de Proteção de Dados (*Data Protection Officer* ou DPO) também é fundamental para o sucesso da governança dos dados e atendimento às regulações vigentes.

Este artigo (o 14º) toca num ponto central para qualquer framework de governança de IA: a responsabilidade institucional não se esgota na escolha da tecnologia, mas exige a construção de estruturas internas capazes de sustentar o ciclo de vida completo dos dados e sistemas adotados. Na prática, isso significa que a governança de IA não pode ser tratada como um projeto pontual de TI, mas como uma função corporativa contínua sob um programa de gestão e melhoria contínua, que contemple, não apenas os benefícios que a tecnologia proporciona, mas também o gerenciamento dos riscos regulatórios que o uso desta pode impactar em uma instituição de saúde.

A governança de IA deve contemplar ao menos 4 dimensões: (1) inventário e classificação de sistemas de IA; 100% das soluções devem ser catalogadas, ter o risco classificado e um responsável técnico designado; (2) gestão do ciclo de vida do modelo e dos dados, monitorando continuamente o desempenho destes, estabelecendo gatilhos para revisão e recertificação, e mantendo documentação técnica atualizada; (3) gestão de fornecedores e terceiros, com atenção para cláusulas contratuais e diligências contemplarem critérios técnicos de IA; (4) gestão de incidentes envolvendo IA, estabelecendo fluxos de resposta, notificação e remediação; (5) gestão dos investimentos e custos no implementação e manutenção dos modelos, tendo em vista, não apenas o retorno relacionada à eficiência obtida, mas também os custos por consumo de tokens para funcionamento dos modelos de IA nas instituições de saúde.

E vale lembrar que a governança de IA não é uma atribuição exclusiva da área técnica. A comissão de IA, além de médicos e profissionais de TI, deve incluir representantes de Compliance, Jurídico, Privacidade e Gestão de Riscos.

O desafio da IA demanda múltiplos expertises, e as organizações do ecossistema de saúde devem atuar para atender os frameworks e regulamentações já existentes, como a Resolução CFM nº 2.454/2026 e a LGPD, bem como se preparar para aquelas que ainda virão, lembrando dos trabalhos em andamento pela ANS e pela SUSEP.

Fonte: https://sistemas.cfm.org.br/normas/arquivos/resolucoes/BR/2026/2454_2026.pdf

(19.05.2026)