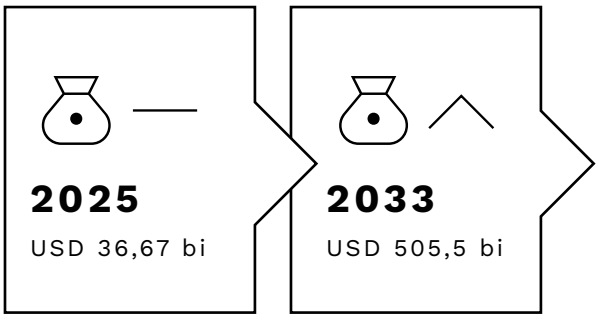
INTELIGÊNCIA ARTIFICIAL (“IA”) NA SAÚDE

A Inteligência Artificial tem transformado profundamente o setor de saúde, impulsionando o desenvolvimento de soluções tecnológicas capazes de monitorar, diagnosticar, informar e apoiar a tomada de decisão clínica com precisão crescente. Essas soluções abrangem um espectro amplo de aplicações — de dispositivos vestíveis (*wearables*) e equipamentos de diagnóstico por imagem a chatbots e assistentes virtuais voltados a orientar pacientes, organizar informações de saúde e dar suporte a profissionais e instituições da área.

De acordo com o relatório *‘AI in Healthcare Market Size & Share | Industry Report, 2033’*, o mercado global de IA na saúde foi avaliado em aproximadamente USD 36,67 bilhões em 2025 e deverá alcançar USD 505,59 bilhões até 2033, crescendo a uma taxa composta anual de 38,90%.



No plano regulatório internacional, a Organização Mundial da Saúde (OMS) publicou, em 2023, o documento Regulatory Considerations on Artificial Intelligence for Health, que estabelece seis pilares fundamentais para a regulação da IA na saúde:

- documentação e transparência ao longo de todo o processo de desenvolvimento, para o rastreamento das etapas e decisões adotadas
- gestão de riscos e ciclo de vida dos sistemas de IA, por meio de uma abordagem que abranja desde o desenvolvimento pré-mercado até a vigilância pós-comercialização e o gerenciamento de mudanças
- uso pretendido e validação analítica e clínica, com documentação transparente e realização de validação externa independente, calibrada ao nível de risco da aplicação
- qualidade dos dados e mitigação de vieses e erros

privacidade e proteção de dados, com implementação de programas de conformidade que considerem os riscos de privacidade e cibersegurança

engajamento e colaboração entre os diferentes atores envolvidos

Já em relatório denominado 'Ética e Governança da Inteligência Artificial para a Saúde (Ethics & Governance of Artificial Intelligence for Health', de 2021, a OMS descreveu os seis princípios consensuais que devem ser observados para garantir que a IA funcione em benefício da população:

- Proteção da autonomia
- Promoção da segurança e bem-estar humanos
- Garantia da transparência
- Promoção da responsabilização
- Garantia da equidade
- Promoção de ferramentas responsivas e sustentáveis

No Brasil, embora o Marco Legal da Inteligência Artificial (PL 2338/2023) ainda esteja em tramitação, o uso da IA na saúde já encontra amparo regulatório em diversos diplomas normativos, em especial, os seguintes:

a Lei Geral de Proteção de Dados ("LGPD"), que classifica os dados de saúde como dados pessoais sensíveis, impondo bases legais mais restritas para o seu tratamento e vedando o compartilhamento entre controladores para fins econômicos;

a RDC Anvisa nº 751/2022, que enquadra os softwares com finalidade clínica como dispositivos médicos; e

a Resolução CFM nº 2.454/2026, que estabelece normas para a pesquisa, o desenvolvimento, a governança, a auditoria, o monitoramento, a capacitação e o uso responsável de soluções de IA na medicina.

Diante desse cenário, o time de Tecnologia e Inovação do Cescon Barrieu elaborou o presente documento com o objetivo de apresentar os principais benefícios e riscos associados aos sistemas de IA aplicados à saúde, bem como os cuidados que devem ser observados sob a perspectiva jurídica, à luz da legislação brasileira e considerando os diferentes formatos de aplicação.

1. PRINCIPAIS APLICAÇÕES E BENEFÍCIOS DAS FERRAMENTAS DE IA NA SAÚDE

Automatização de Fluxos: ganho de eficiência operacional e administrativa por meio da automatização de fluxos de trabalho, como, por exemplo, elaboração de anotações clínicas, agendamento de consultas, faturamento, triagem de pacientes, gestão de documentos clínicos, processamento de autorizações e sumarização de prontuários.

Cirurgias robóticas: maior precisão em procedimentos cirúrgicos, viabilização de técnicas menos invasivas, telecirurgia e ampliação do acesso à saúde.

Auxílio diagnóstico e farmacológico: análise de grandes volumes de dados clínicos, exames laboratoriais e imagens médicas com alta velocidade e precisão, oferecendo suporte a profissionais da saúde na formulação de diagnósticos e na indicação precisa de medicamentos e respectivas posologias, com base em evidências científicas, protocolos clínicos, ferramentas de deep learning e na integração de informações clínicas dos pacientes.

Monitoramento e prevenção: integração com dispositivos de saúde para monitoramento contínuo de condições clínicas, prevenção de doenças, detecção de enfermidades infecciosas e apoio à tomada de decisões clínicas, além da geração de insights para o controle de doenças crônicas e a melhoria da qualidade de vida dos pacientes.

Sistematização de informações: armazenamento e análise de grandes volumes de dados, permitindo a geração de insights clínicos e uma visão mais abrangente sobre possíveis diagnósticos e condições de saúde.

Assistência virtual e ampliação do acesso: utilização de chatbots, telemedicina, aplicativos e plataformas digitais de triagem capazes de responder a dúvidas sobre medicamentos e sintomas, fornecer orientações de saúde e apoiar a tomada de decisão no cuidado pessoal do paciente, contribuindo para levar atendimento e orientação médica a regiões com menor infraestrutura ou disponibilidade de profissionais especializados.

2. PRINCIPAIS RISCOS RELACIONADOS AO USO DE FERRAMENTAS DE IA

Dados e privacidade: riscos associados ao tratamento irregular de dados pessoais sensíveis de pacientes, a ataques cibernéticos que exponham informações de saúde, bem como ao uso secundário de dados clínicos para fins comerciais sem a devida transparência. Em relação às IAs que operam por meio de Modelos de Linguagem de Grande Escala (“LLMs”), um dos riscos é o "prompt injection" - inserção de instruções maliciosas para manipular o comportamento do sistema de IA, fazendo com que execute funções não programadas - incluindo a extração não autorizada de informações confidenciais, como registros de pacientes, históricos clínicos e dados proprietários do sistema processados no contexto do modelo.

Qualidade e confiabilidade dos algoritmos: viés algorítmico decorrente de sistemas treinados com dados pouco representativos, que podem gerar diagnósticos menos precisos para grupos minoritários ou populações de países em desenvolvimento; erros de diagnóstico com consequências clínicas graves, incluindo falsos positivos e falsos negativos, especialmente quando os modelos são aplicados em contextos distintos daqueles em que foram treinados; e alucinações em modelos de linguagem aplicados à saúde, que produzem respostas plausíveis, porém incorretas.

Responsabilidade e ética: a complexidade de muitos algoritmos, especialmente os baseados em aprendizado profundo (deep learning), dificulta a compreensão sobre como as decisões são tomadas. Isso levanta questões sobre confiabilidade e auditabilidade, bem como falta de transparência sobre como decisões clínicas são tomadas pelos algoritmos (efeito "caixa-preta"); risco de transferência de decisões médicas complexas para sistemas automatizados sem supervisão humana adequada; e prejuízo à autonomia do paciente no processo de tomada de decisão.

Regulação e governança: número reduzido de países com estratégias nacionais específicas para IA na saúde; ausência de padrões internacionais unificados de certificação e auditoria de sistemas; e dificuldade de validação clínica rigorosa antes da adoção em larga escala.

Riscos sistêmicos e operacionais: falhas técnicas em sistemas críticos de suporte à decisão clínica; dependência da infraestrutura tecnológica; desatualização acelerada dos modelos sem processos adequados de retreinamento e validação; e utilização da IA por agentes mal-intencionados para a prática de fraudes mais sofisticadas no âmbito de planos e operadoras de saúde.

3. CUIDADOS NO USO DE FERRAMENTAS DE IA SOB A PERSPECTIVA JURÍDICA

As obrigações aplicáveis aos agentes de IA variam conforme a natureza de sua atuação na cadeia de valor do sistema. Para fins de maior aderência ao cenário regulatório brasileiro, adotam-se as definições previstas no PL 2338/2023 (mesmo que ainda não em vigor): (i) desenvolvedor, pessoa natural ou jurídica, de natureza pública ou privada, que desenvolva sistema de IA, diretamente ou por encomenda, com vistas à sua colocação no mercado ou à sua aplicação em serviço por ela fornecido, sob seu próprio nome ou marca, a título oneroso ou gratuito; (ii) distribuidor, pessoa natural ou jurídica, de natureza pública ou privada, que disponibilize e distribua sistema de IA para que terceiro o aplique, a título oneroso ou gratuito; e (iii) aplicador, pessoa natural ou jurídica, de natureza pública ou privada, que empregue ou utilize, em seu nome ou benefício, sistema de IA, inclusive configurando, mantendo ou apoiando com o fornecimento de dados para a operação e o monitoramento do sistema.

	DESENVOLVEDOR	DISTRIBUIDOR	APLICADOR
LGPD	X	X	X
PL 2338/2023	X	X	X
RESOLUÇÃO RDC ANVISA Nº 751/2022	X	X	-
RESOLUÇÃO CFM Nº 2454/2026	X*	X*	X

*aplicável de forma indireta via requisitos de conformidade

3.1. LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709/2018), “LGPD”

A LGPD aplica-se a qualquer operação de tratamento de dados pessoais realizada por pessoa natural ou jurídica, de direito público ou privado, independentemente do meio, do país de origem ou do país onde estejam localizados os dados, desde que o tratamento ocorra no Brasil, que a atividade de coleta tenha sido realizada em território nacional, ou que os dados tratados sejam de indivíduos que se encontrem no país. Nesse sentido, suas obrigações estendem-se a desenvolvedores, distribuidores e aplicadores dos sistemas IA.

No contexto de sistemas de IA aplicados à saúde, sua incidência é especialmente relevante: o desenvolvimento, a distribuição e a utilização dessas soluções envolvem, invariavelmente, dados pessoais sensíveis — como prontuários, diagnósticos, exames e históricos clínicos —, que recebem proteção reforçada pela lei. Isso significa que toda a cadeia de IA em saúde, do treinamento de modelos com bases de dados de pacientes à geração de recomendações clínicas em tempo real, está sujeita às exigências da LGPD, incluindo a necessidade de base legal adequada, a adoção de medidas de segurança compatíveis com a sensibilidade dos dados e a garantia dos direitos dos titulares, como acesso, correção e revisão de decisões automatizadas.

No que se refere às bases legais, o uso de IA na área da saúde apresenta desafios adicionais, uma vez que o tratamento de dados pessoais sensíveis somente é permitido nas hipóteses taxativas do art. 11 da LGPD. Assim, todas as atividades de tratamento — desde o treinamento dos modelos até a sua utilização para fins diagnósticos ou administrativos que envolvam o compartilhamento de informações de saúde — devem estar amparadas em uma das bases legais previstas no referido dispositivo. A seguir, indicamos algumas das hipóteses com maior aderência às possíveis aplicações na área da saúde:

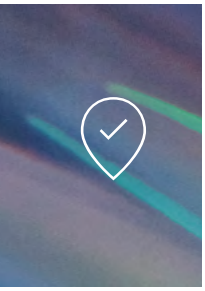
BASE LEGAL

CONSENTIMENTO

Consentimento específico e destacado, para finalidades específicas

APLICABILIDADE EM IA NA SAÚDE

Exige que o titular compreenda que seus dados serão processados por sistema de IA; deve ser granular e revogável; exige gestão que permita a revogação.



BASE LEGAL

EXERCÍCIO REGULAR DE DIREITOS

Inclusive em contratos

APLICABILIDADE EM IA NA SAÚDE

Aplicável quando o tratamento dos dados de saúde ocorrer exclusivamente para a execução/o cumprimento de um contrato.

BASE LEGAL

PROTEÇÃO DA VIDA

Geralmente aplicável em contexto de situação de risco iminente

APLICABILIDADE EM IA NA SAÚDE

Aplicável em sistemas de triagem e emergência

BASE LEGAL

TUTELA DA SAÚDE

Exclusivo para profissional de saúde, serviços de saúde ou autoridade sanitária

APLICABILIDADE EM IA NA SAÚDE

Base mais usual para IA clínica; operador deve ser ou atuar sob supervisão de serviço de saúde

O desenvolvimento de sistemas de machine learning pressupõe, por definição, a necessidade de treinamento a partir de conjuntos de dados. Quando esses dados envolvem informações pessoais sensíveis — como dados de saúde —, o leque de bases legais disponíveis se estreita: o uso do legítimo interesse como base legal de tratamento é expressamente vedado, e as demais hipóteses que permanecem aplicáveis, como a tutela da saúde, a proteção da vida e o exercício regular de direitos, têm escopo limitado e dificilmente se prestam a justificar o treinamento de modelos em larga escala. Na prática, resta ao desenvolvedor recorrer ao consentimento do titular — o que, contudo, impõe um desafio técnico-jurídico de difícil solução: o consentimento deve ser revogável a qualquer momento, mas os meios técnicos para "desensinar" um modelo já treinado são, no estado atual da tecnologia, inexistentes, o que torna a revogação efetiva uma obrigação de cumprimento incerto.

Além disso, considerando que sistemas de IA frequentemente operam por meio de decisões automatizadas, o agente deve assegurar, de forma permanente e operacional, a possibilidade de revisão humana das decisões que afetem os interesses dos titulares.

O tratamento de dados de saúde por sistemas de IA configura, por natureza, uma operação de alto risco, o que torna a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (“RIPD”) uma medida essencial. No contexto de IA aplicada à saúde, esse relatório deve ir além da avaliação genérica

de riscos e contemplar especificamente: (i) os riscos de vieses algorítmicos com potencial impacto sobre diagnósticos e tratamentos; (ii) os riscos inerentes a decisões automatizadas com efeitos diretos sobre a saúde do titular; (iii) os riscos de vazamento de dados com alto potencial discriminatório; e (iv) as medidas de auditabilidade e rastreabilidade adotadas nos processos do sistema.

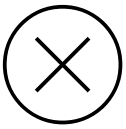
Também é importante destacar que, em 25 de fevereiro de 2026, a ANPD passou por uma transformação institucional histórica: a Lei nº 15.352/2026 converteu formalmente a Autoridade Nacional de Proteção de Dados em uma agência reguladora plenamente independente (Agência Nacional de Proteção de Dados), conferindo-lhe autonomia funcional, técnica, decisória, administrativa e financeira.

Seus poderes de fiscalização também foram significativamente ampliados: os fiscais da agência podem agora determinar a interdição de estabelecimentos, equipamentos e instalações, bem como o sequestro de bens e produtos, contando com o apoio de polícia federal ou estadual em caso de resistência.

A lei criou ainda 200 cargos especializados em regulação e fiscalização da proteção de dados, a serem preenchidos por concurso público, ampliando substancialmente a capacidade técnica e fiscalizatória da agência. Nesse contexto de fortalecimento institucional, a ANPD tem atuado de forma ativa na definição de sua agenda regulatória e de fiscalização, com foco específico em inteligência artificial e dados de saúde.

A Agenda Regulatória 2025–2026 — publicada em 11 de dezembro de 2024, por meio da Resolução CD/ANPD nº 23/2024 — identificou a inteligência artificial e os dados sensíveis, incluindo dados biométricos e de saúde, entre suas 16 áreas temáticas prioritárias para a fase normativa.

Mais recentemente, o Mapa de Temas Prioritários 2026–2027 — publicado em 24 de dezembro de 2025, por meio da Resolução CD/ANPD nº 30/2025 — elencou a inteligência artificial e as tecnologias emergentes como um dos quatro eixos centrais de fiscalização para o próximo biênio. Em conjunto, esses desdobramentos indicam que a ANPD dispõe agora do mandato institucional, dos instrumentos de fiscalização e da capacidade operacional necessários para examinar o cumprimento da LGPD com rigor sem precedentes, tornando a conformidade proativa uma prioridade estratégica para todos os agentes da cadeia de inteligência artificial na área da saúde.



VEDAÇÕES

- vender, licenciar ou monetizar bases de dados de saúde;
- compartilhar dados de saúde com parceiros comerciais em troca de qualquer forma de remuneração ou contraprestação; e/ou
- participar de arranjos de data brokerage que envolvam dados sensíveis.

3.2. MARCO LEGAL DA IA (PL Nº 2338/2023)

O Marco Legal da IA (se e quando aprovado) instituirá um regime diferenciado de obrigações para sistemas de IA classificados como de alto risco — categoria que abrange expressamente aplicações voltadas ao auxílio diagnóstico e a procedimentos médicos. O Marco Legal da IA distribui essas obrigações ao longo de toda a cadeia de agentes envolvidos no desenvolvimento, na distribuição e na aplicação dos sistemas, com especial ênfase na rastreabilidade, na mitigação de vieses e na responsabilização algorítmica.

OBRIGAÇÕES GERAIS	SISTEMAS DE ALTO RISCO (INCLUI IA NA SAÚDE)
TODOS OS AGENTES DA CADEIA	
• Garantir segurança dos sistemas e direitos dos afetados • Cooperar e fornecer informações à autoridade • Incluir identificador em conteúdo sintético gerado • Comunicar à autoridade a ocorrência de grave incidente	• Informar procedimentos para exercício de direitos dos titulares • Comunicar risco ou impacto inesperado à autoridade e demais agentes da cadeia
DESENVOLVEDORES	
• Impedir uso do sistema para propósitos vedados • Publicar sumário sobre conteúdos protegidos utilizados no desenvolvimento • Remunerar titulares de propriedade intelectual utilizada no treinamento **SISTEMAS DE IA DE PROPÓSITO GERAL / IA GENERATIVA:** • Realizar avaliação preliminar de risco • Documentar modelo, testes, riscos e conjuntos de dados • Elaborar documentação técnica e instruções de utilização	• Manter registro das medidas de governança • Registrar a operação do sistema • Realizar testes de segurança • Fornecer informações para interpretar os resultados gerados • Mitigar e prevenir vieses discriminatórios • Compartilhar avaliações com a autoridade setorial ⚑ Realizar Avaliação de Impacto Algorítmico (AIA)

• Conceber sistemas de forma sustentável • Cooperar para mitigação de riscos	
APLICADORES	
	• Documentar todas as etapas do ciclo de vida do sistema • Avaliar os resultados da utilização do sistema • Documentar testes de confiabilidade e segurança • Documentar grau de supervisão humana efetivamente mantido • Fornecer informações para interpretar resultados • Mitigar e prevenir vieses discriminatórios ⚑ Realizar Avaliação de Impacto Algorítmico (AIA)
DISTRIBUIDORES	
	• Apoiar e verificar o cumprimento das medidas de governança pelos demais agentes da cadeia

⚑

AVALIAÇÃO DE IMPACTO ALGORÍTMICO (“AIA”)

Obrigação exigida de Desenvolvedores e Aplicadores. A AIA deve identificar, analisar e mitigar riscos algorítmicos, com atenção a: vieses que possam distorcer diagnósticos; decisões automatizadas com efeito sobre a saúde do titular; e impactos sobre grupos vulneráveis. Além do mapeamento de riscos, a avaliação deve também abordar as dimensões técnicas do desenvolvimento e da implantação do sistema — em especial, o grau em que a ferramenta é capaz de fornecer explicabilidade e transparência em relação aos seus resultados e à lógica de tomada de decisão. Esse requisito representa um desafio prático considerável: conforme discutido anteriormente no contexto dos riscos

relacionados a dados e privacidade, os modelos de aprendizado profundo são inerentemente opacos, tornando difícil — e, em algumas arquiteturas, atualmente impossível — prestar contas integralmente de como um determinado resultado foi alcançado.

O AIA deve, portanto, não apenas identificar essa limitação, mas também documentar as medidas de mitigação adotadas, tais como o uso de técnicas de interpretabilidade post-hoc, protocolos de supervisão humana e os limites dentro dos quais o sistema pode ser implantado com segurança. Desenvolvedores devem compartilhar as avaliações com a autoridade setorial competente.

3.3. ANVISA RDC NO. 751/2022 (“RDC 751”)

A RDC 751 estabelece as regras de classificação de risco, regimes de notificação e registro e requisitos de rotulagem aplicáveis aos dispositivos médicos no Brasil. A norma enquadra como *Software as a Medical Device* (“SaMD”) todo software que desempenhe funções médicas de forma independente — isto é, sem estar incorporado ao hardware de um dispositivo médico — incluindo aplicativos móveis. Softwares limitados a funções administrativas, operacionais ou informativas genéricas permanecem fora do escopo da RDC 751.

O critério determinante para esse enquadramento é a finalidade pretendida do software. Quando destinado a **diagnóstico, prevenção, monitoramento, tratamento ou apoio à decisão clínica**, o sistema passa a ser considerado dispositivo médico e deve ser regularizado perante a Agência Nacional de Vigilância Sanitária (“Anvisa”) antes de sua comercialização. Softwares destinados exclusivamente a investigações clínicas formais estão isentos de notificação ou registro, desde que não sejam comercializados nem utilizados para outros fins. Essa hipótese não se confunde com o uso rotineiro de softwares por médicos para apoio ao diagnóstico, que configura finalidade médica direta e sujeita o sistema à regularização como SaMD.

A fronteira entre essas categorias, contudo, pode ser tênue. A Anvisa pode reenquadrar o produto caso entenda que existe finalidade médica implícita, ainda que não declarada pelo fabricante.

A RDC 751 classifica os dispositivos médicos em quatro classes de risco, que determinam o regime regulatório aplicável. Dispositivos das Classes I e II estão sujeitos a notificação, enquanto dispositivos das Classes III e IV exigem registro prévio junto à Anvisa.

Para SaMDs, aplica-se a **Regra 11 de classificação**, que define o enquadramento regulatório conforme a finalidade do software e o potencial impacto clínico das decisões por ele suportadas:

	REGIME REGULATÓRIO	EXEMPLO DE APLICAÇÃO EM IA NA SAÚDE
CLASSE I (BAIXO RISCO)	**NOTIFICAÇÃO**	Softwares administrativos sem impacto clínico direto, como sistemas de agendamento, gestão logística hospitalar ou organização de fluxos operacionais

REGIME REGULATÓRIO

NOTIFICAÇÃO

EXEMPLO DE APLICAÇÃO EM IA NA SAÚDE

Sistemas de apoio à decisão clínica sem impacto crítico imediato, como ferramentas de análise de exames ou monitoramento de processos fisiológicos não vitais

REGIME REGULATÓRIO

REGISTRO

EXEMPLO DE APLICAÇÃO EM IA NA SAÚDE

Sistemas de IA cujas recomendações possam influenciar decisões clínicas críticas, incluindo softwares que auxiliem diagnósticos que possam levar a deterioração grave da saúde ou orientar intervenções cirúrgicas, bem como monitoramento de parâmetros vitais críticos

REGIME REGULATÓRIO

REGISTRO

EXEMPLO DE APLICAÇÃO EM IA NA SAÚDE

Sistemas de IA cujas decisões ou recomendações possam resultar em morte ou deterioração irreversível da saúde do paciente, como algoritmos utilizados em decisões clínicas altamente críticas

3.4. RESOLUÇÃO CFM Nº 2.454/2026

A Resolução CFM nº 2.454/2026 ("Resolução CFM IA"), por sua vez, estabelece diretrizes para a pesquisa, desenvolvimento, governança, auditoria, monitoramento e uso responsável de sistemas de IA na medicina. A norma disciplina o uso dessas tecnologias na prática médica e estrutura um modelo regulatório baseado em supervisão humana, governança institucional e transparência tecnológica.

A Resolução CFM IA parte de três premissas centrais:

- Supervisão humana obrigatória: a IA é reconhecida exclusivamente como ferramenta de apoio à prática médica. O médico permanece responsável pelas decisões clínicas, diagnósticas, terapêuticas e prognósticas, não podendo delegar tais decisões a sistemas automatizados.
- Direitos e autonomia do paciente: o paciente deve ser informado quando sistemas de IA forem utilizados como apoio relevante em seu cuidado. A comunicação de diagnósticos, prognósticos ou decisões terapêuticas não pode ser realizada exclusivamente por sistemas automatizados, e o paciente mantém o direito de recusar o uso de IA em seu atendimento.
- Governança institucional e avaliação de risco: instituições de saúde devem implementar mecanismos internos de governança para o uso de IA, incluindo avaliação preliminar de risco, monitoramento contínuo das soluções e adoção de medidas para prevenir vieses discriminatórios, assegurar transparência e garantir a proteção de dados de saúde. Nesse sentido, a Resolução CFM sobre IA reforça expressamente a obrigação de realizar uma Avaliação de Impacto Algorítmico. O documento define a AIA como uma análise contínua dos impactos de um sistema de inteligência artificial, estabelecendo que ela "deve ser documentada e periodicamente atualizada" com vistas à identificação de medidas preventivas e mitigadoras, em alinhamento direto com o arcabouço previsto no Projeto de Lei nº 2.338/2023.

Embora a Resolução CFM IA se dirija diretamente a médicos e instituições de saúde, seus requisitos produzem efeitos indiretos relevantes para desenvolvedores e distribuidores de tecnologias de IA, que passam a ser demandados por maior transparência, auditabilidade e interoperabilidade de seus sistemas.

Quadro-resumo de obrigações por agente:

PRINCIPAIS OBRIGAÇÕES / IMPLICAÇÕES

- Utilizar sistemas de IA exclusivamente como ferramenta de apoio
- Exercer julgamento clínico crítico sobre recomendações da IA
- Registrar o uso de IA no prontuário do paciente
- Comunicar falhas ou riscos às instâncias competentes
- Manter-se atualizado quanto às capacidades, limitações e vieses dos sistemas
- Respeitar a autonomia e os direitos do paciente

CONSEQUÊNCIAS DO DESCUMPRIMENTO

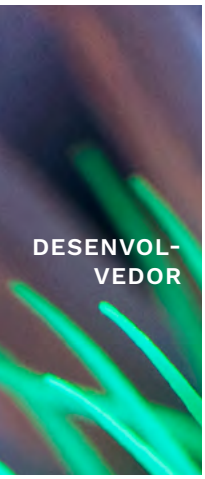
Sanções ético-disciplinares perante o Conselho Regional de Medicina (art. 8º), sem prejuízo de responsabilização civil e penal. O médico permanece integralmente responsável pelos atos praticados com auxílio de IA (art. 7º).

PRINCIPAIS OBRIGAÇÕES / IMPLICAÇÕES

- Realizar avaliação preliminar de risco antes da adoção da solução de IA
- Implementar governança interna (transparência, auditoria e mitigação de vieses)
- Criar Comissão de IA e Telemedicina quando utilizar sistemas próprios
- Garantir interoperabilidade e monitoramento contínuo das soluções
- Assegurar proteção de dados e segurança da informação
- Colaborar com órgãos reguladores e de fiscalização

CONSEQUÊNCIAS DO DESCUMPRIMENTO

Fiscalização e supervisão pelo Conselho Regional de Medicina da jurisdição (art. 15). Descumprimento das obrigações de governança pode ensejar medidas administrativas e responsabilização da diretoria técnica (arts. 9º e 14).



PRINCIPAIS OBRIGAÇÕES / IMPLICAÇÕES

- Fornecer documentação técnica clara sobre funcionamento, riscos e limitações do sistema
- Garantir auditabilidade e explicabilidade das soluções
- Adotar princípios de privacy by design e privacy by default
- Disponibilizar suporte para atualização, retreinamento e monitoramento do sistema
- Colaborar com autoridades regulatórias e instituições de saúde

CONSEQUÊNCIAS DO DESCUMPRIMENTO

Efeitos indiretos: sistemas que não atendam aos requisitos de transparência, auditabilidade e explicabilidade podem ser recusados ou descontinuados por instituições médicas. Eventual responsabilização civil por falhas atribuíveis ao sistema (art. 7º, §2º, c/c legislação aplicável).

DISTRIBUIDOR

PRINCIPAIS OBRIGAÇÕES / IMPLICAÇÕES

- Disponibilizar informações completas sobre o sistema distribuído
- Garantir que a solução atenda aos requisitos regulatórios e éticos aplicáveis
- Atuar na intermediação entre desenvolvedor e instituição médica
- Colaborar com instituições e órgãos de controle em caso de incidentes ou falhas

CONSEQUÊNCIAS DO DESCUMPRIMENTO

Efeitos indiretos: risco de recusa ou descontinuação do sistema por instituições médicas caso a solução não atenda aos requisitos regulatórios e éticos. Eventual responsabilização solidária por falhas na cadeia de fornecimento, conforme legislação aplicável.

> Ao paciente, titular de direitos, fica garantido o direito à informação sobre o uso de IA em seu cuidado, o direito de recusar o uso de sistemas de IA, o direito à privacidade e confidencialidade de seus dados de saúde, o direito à segunda opinião médica, e o direito ao consentimento específico para intervenções experimentais.

A Resolução CFM IA cria um ambiente regulatório no qual médicos e instituições passam a exigir de fornecedores de tecnologia maior transparência, explicabilidade e segurança das soluções de IA. Desenvolvedores e distribuidores que anteciparem esses requisitos — incorporando-os desde a fase de concepção do produto — tendem a encontrar menores barreiras regulatórias e maior aceitação no mercado de saúde.

4. CONCLUSÃO

A conformidade com um dos diplomas legais mencionados acima não substitui, mas se soma às obrigações constantes dos demais. Na prática, um mesmo software de IA poderá ter que cumprir, simultaneamente com o seguinte:

- notificação ou registro na Anvisa, conforme sua classificação de risco;
- conformidade com a LGPD no tratamento de dados de saúde, incluindo base legal adequada, avaliação de impacto e limitações ao compartilhamento de dados;
- conformidade com o Marco Legal da IA, quando este entrar em vigor – ou de forma antecipada, como medida de boa prática; e
- adequação aos requisitos de governança, auditoria e transparência previstos pela Resolução CFM, que também estabelece classificação própria de risco para sistemas de IA na medicina.

Quanto a possíveis responsabilizações, o tratamento irregular de dados pessoais pode gerar sanções administrativas pela Agência Nacional de Proteção de Dados (“ANPD”) nos termos da LGPD, enquanto o descumprimento das normas do Marco Legal da IA também sujeitará o inadimplente às respectivas sanções. A comercialização de software com finalidade médica sem a devida regularização sanitária, por sua vez, configura infração sanitária, sujeita às penalidades previstas na legislação aplicável ao setor, em especial a Lei nº 6.437/1977, enquanto a inobservância das normas do CFM pode expor o médico a sanções éticas perante o Conselho Regional de Medicina, sem prejuízo de eventuais responsabilidades civil e penal.

A combinação de inteligência artificial e medicina não é apenas possível, mas altamente promissora. Aqueles que optam por atuar nesse espaço, contudo, devem estar preparados para assumir um ônus regulatório estruturado e multifacetado — que é ativamente fiscalizado e segue em constante expansão.

NOSSA EQUIPE

Se você tiver qualquer dúvida jurídica relacionada à IA na saúde, não hesite em entrar em contato com a nossa equipe

ESTHER FLESCH
SÓCIA
esther.flesch@cesconbarrieu.com.br

JULIA PAZOS
SÓCIA
julia.pazos@cesconbarrieu.com.br

TANIA LIBERMAN
SÓCIA
tania.liberman@cesconbarrieu.com.br

ANA LUIZA CALIL
OF COUNSEL
analuiza.calil@cesconbarrieu.com.br

PEDRO GUERRA
ASSOCIATE
pedro.guerra@cesconbarrieu.com.br

LAIS HORTA
ASSOCIADA
lais.horta@cesconbarrieu.com.br

ANA CAROLINA SCHINAIDER
ASSOCIADA
anacarolina.schinaider@cesconbarrieu.com.br