



saude.dev

Sete documentos para organizar o uso de IA no consultório

DOCUMENTO 4 DE 7

Questionário do fornecedor

v1.0 · setembro de 2026

Carlos Avila · médico · informática em saúde e proteção de dados

saude.dev/kits/ia-no-consultorio

Doze perguntas para enviar a quem vende IA ao seu serviço — antes de assinar e uma vez por ano depois disso. Cada pergunta diz **por que** é feita, com o dispositivo da Resolução CFM nº 2.454/2026 ou da LGPD, e o que é uma resposta aceitável.

NOTA

Este documento é material informativo e educacional, escrito por médico com atuação em informática em saúde e proteção de dados. Não é orientação jurídica, não substitui parecer do CRM nem de assessoria jurídica, e não assegura, por si, o cumprimento de norma alguma. Adapte o texto ao seu serviço e revise com quem responde tecnicamente por ele antes de usar. As citações seguem o texto oficial da Resolução CFM nº 2.454/2026; onde este kit propõe uma tradução operacional nossa, o trecho vem marcado como *(prática recomendada — não é exigência literal)*.

Como usar este documento

Este é o documento 4 de 7 do kit. Ele funciona sozinho, mas conversa com os outros seis (mapa ao final).

- 1 Envie o e-mail da seção 2 com as doze perguntas da seção 3 em anexo. Dê quinze dias.
- 2 Avalie cada resposta na ficha da seção 4. Quatro perguntas são **bloqueantes**: sem resposta aceitável, não contrate.
- 3 Anexe as respostas ao contrato e marque a reavaliação anual (documento 6, calendário).

1. Como usar o questionário

Quando. Antes de contratar qualquer sistema de IA que receba dado de paciente ou influencie decisão clínica; e anualmente, ou quando o fornecedor anunciar mudança relevante de modelo, de infraestrutura ou de termos.

Por quê. O médico tem o direito de “recusar a utilização de sistemas de IA que não apresentem validação científica ou certificação regulatória adequada” (art. 3º, III) e o dever de “utilizar apenas sistemas de IA que atendam às normas e regulamentações vigentes” (art. 4º, IV). Para exercer esse direito e cumprir esse dever, é preciso perguntar. As respostas também alimentam a avaliação preliminar do documento 1 e a política de IA do documento 5.

Regras práticas *(prática recomendada — não é exigência literal)*:

- 1 Quinze dias para responder. Fornecedor sério responde em menos.
- 2 A resposta vira anexo do contrato, ou declaração assinada, ou ao menos e-mail arquivado com data. Resposta só por telefone não conta.
- 3 Sem resposta aceitável a uma pergunta bloqueante (4, 5, 7 e 8), não contrate. Se já usa o sistema, suspenda o envio de dados identificáveis até resolver.
- 4 Guarde a ficha preenchida (seção 4) junto do inventário do documento 1.
- 5 Vale para “IA embutida” também: se o seu prontuário eletrônico ganhou um botão de IA, o fornecedor do prontuário responde às mesmas perguntas.

2. E-mail modelo

Assunto: Questionário sobre o sistema de IA [NOME DO SISTEMA] — Resolução CFM 2.454/2026

Prezados,

Somos [NOME DO SERVIÇO] e [estamos avaliando a contratação / utilizamos] o sistema

[NOME DO SISTEMA]. A Resolução CFM nº 2.454/2026, em vigor desde 26/08/2026, exige que serviços médicos avaliem o risco dos sistemas de IA que usam, registrem seu uso e assegurem a proteção dos dados dos pacientes.

Para isso, pedimos resposta por escrito às doze perguntas em anexo até [DATA – 15 DIAS]. As respostas serão anexadas ao contrato e reavaliadas anualmente.

Quatro perguntas (4, 5, 7 e 8) são condição para a contratação ou continuidade. Se alguma informação for confidencial, indiquem e proporemos acordo de sigilo.

Atenciosamente,

[NOME], [CARGO – ex.: responsável técnico], [NOME DO SERVIÇO]

[TELEFONE / E-MAIL]

3. As doze perguntas

3.1 Bloco A – Finalidade, validação e limitações

Q1 Nível de risco

Qual nível de risco (baixo, médio, alto) vocês atribuem ao sistema, segundo o Anexo II da Resolução CFM nº 2.454/2026, e para quais finalidades de uso essa classificação vale?

POR QUE PERGUNTAMOS

O art. 13 diz que os níveis de risco “deverão ser informados ao usuário”. O nível que o fornecedor declara entra na avaliação preliminar do serviço (documento 1).

RESPOSTA ACEITÁVEL

Um nível declarado, com a finalidade delimitada por escrito. “Depende do uso” sem detalhar é resposta incompleta.

Q2 Validação científica e situação regulatória

Que evidência de validação existe (estudos, métricas de desempenho, população testada)? O sistema é registrado ou notificado como dispositivo médico junto à ANVISA? Se não, por quê?

POR QUE PERGUNTAMOS

Direito de recusar sistemas “sem validação científica ou certificação regulatória adequada” (art. 3º, III); dever de usar apenas sistemas que atendam às normas (art. 4º, IV); validação e “testes exaustivos” (art. 9º).

RESPOSTA ACEITÁVEL

Referência a estudo ou relatório técnico acessível, com métricas e população. Sobre a ANVISA: situação clara (“regularizado sob nº X” ou “não é dispositivo médico porque Y”). Silêncio sobre o tema é sinal de alerta.

Q3 Limitações, vieses e populações não testadas

Quais são as limitações conhecidas do sistema? Em que populações, idiomas ou contextos ele foi menos testado ou tem desempenho pior? Como vocês monitoram viés?

POR QUE PERGUNTAMOS

O médico tem direito a informações sobre “limitações, riscos” e “grau de evidência” ([art. 3º, II](#)) e o dever de manter-se informado sobre “vieses” ([art. 4º, III](#)). O Anexo III, I pede relatórios regulares de desempenho, e o Anexo III, II, descontinuar sistemas com viés não eliminável.

RESPOSTA ACEITÁVEL

Uma lista concreta de limitações, com exemplos. “Não há limitações conhecidas” é a pior resposta possível.

3.2 Bloco B – Dados**Q4 Onde os dados ficam e quem os acessa****BLOQUEANTE**

Quais dados de pacientes o sistema recebe? Em que país ficam armazenados e processados? Quem são os subprocessadores (nuvem, modelo de linguagem, transcrição) e onde estão?

POR QUE PERGUNTAMOS

Compartilhamento “apenas quando estritamente necessário”, com “base legal idônea” ([art. 6º, §1º](#)); dever de observar a proteção geral de dados pessoais ([art. 16](#)). Transferência internacional tem regras próprias na LGPD.

RESPOSTA ACEITÁVEL

Lista nominal de subprocessadores e países. Se houver transferência internacional, a base usada. “Usamos provedores de nuvem líderes” não é resposta.

Q5 Uso dos dados para treinar ou melhorar o modelo**BLOQUEANTE**

Os dados dos nossos pacientes (texto, áudio, imagens, prompts) são usados para treinar, validar ou aprimorar o modelo, seu ou de terceiros? Se sim, com que base e como desativar isso?

POR QUE PERGUNTAMOS

O uso de dados para “treinamento, validação e aprimoramento” exige base legal e observância da proteção de dados ([art. 6º, §2º](#); [art. 16](#)). O serviço precisa saber para informar o paciente (documento 3).

RESPOSTA ACEITÁVEL

Por padrão, não usa; ou desativação contratual comprovável (“opt-out” ativo por escrito). Uso para treino sem possibilidade de desativar, em sistema que recebe dado identificável, é motivo para não contratar.

Q6 Retenção e descarte

Por quanto tempo cada tipo de dado (áudio, transcrição, prompt, resultado) fica armazenado? Como é o descarte ao fim do contrato e a devolução dos dados ao serviço?

POR QUE PERGUNTAMOS

Sigilo e confidencialidade “em todas as etapas do ciclo de vida da IA” ([art. 6º](#)) e ciclo de vida do sistema ([art. 9º, §1º](#); Anexo III, VI). O termo de ciência (documento 3) pede prazo de retenção do áudio.

RESPOSTA ACEITÁVEL

Prazos por tipo de dado, exportação em formato aberto e comprovação de exclusão ao término.

Q7 Segurança da informação e incidentes**BLOQUEANTE**

Quais controles de segurança existem (criptografia em trânsito e em repouso, controle de acesso, registro de acessos)? Há certificação ou auditoria independente? Houve incidente de segurança nos últimos 24 meses e como foi tratado?

POR QUE PERGUNTAMOS

Vedado utilizar sistema “que não garanta padrões mínimos de segurança da informação compatíveis com os dados pessoais sensíveis” (art. 6º, §3º); requisitos de segurança e “mecanismos de segurança adequados” (art. 17).

RESPOSTA ACEITÁVEL

Descrição dos controles, relatório de auditoria ou certificação com data, e histórico de incidentes com o que mudou depois. Recusar-se a falar de incidentes é sinal de alerta.

3.3 Bloco C – Autonomia, explicação e controle**Q8 O sistema executa alguma ação sem revisão humana?****BLOQUEANTE**

Existe alguma situação em que o sistema envia, agenda, prescreve, comunica ao paciente ou grava no prontuário sem que um profissional revise antes? Isso é configurável?

POR QUE PERGUNTAMOS

Vedado delegar à IA a comunicação de diagnósticos, prognósticos ou decisões terapêuticas sem mediação humana (art. 5º, §2º); vedado sistema que “restringa ou substitua a autoridade final do médico” (art. 18, §1º); supervisão humana obrigatória (art. 15, parágrafo único).

RESPOSTA ACEITÁVEL

Nenhuma ação clínica sem revisão, ou toda ação automática desligável por configuração e desligada por padrão. Ação clínica automática que não pode ser desligada é motivo para não contratar.

Q9 Explicação e discordância

Como o sistema mostra a origem ou o fundamento de uma sugestão? O médico consegue registrar que discorda, e essa discordância fica salva e é usada por vocês?

POR QUE PERGUNTAMOS

Informações claras sobre “funcionamento” (art. 3º, II); o médico “pode acolher ou rejeitar” a sugestão (art. 18, §2º); contestabilidade e explicabilidade (Exposição de Motivos, princípios II e VI).

RESPOSTA ACEITÁVEL

Interface que mostra fonte, trecho ou critério da sugestão; botão ou campo de discordância que gera registro rastreável.

Q10 Parametrização, logs e auditoria

O que o serviço pode configurar (limiares, modelos, funções ligadas)? Que logs de uso existem, por quanto tempo ficam e como o serviço ou um órgão de fiscalização acessa esses logs?

POR QUE PERGUNTAMOS

Anexo III, V: “capacidade de parametrizações” e “interfaces auditáveis”; Anexo III, VIII: acesso de órgãos de controle a “relatórios de auditoria e logs”; monitoramento e auditoria (art. 9º, §2º).

RESPOSTA ACEITÁVEL

Lista de parâmetros configuráveis; logs com versão do modelo, data, usuário e saída; exportação sob demanda; prazo de guarda compatível com o do prontuário.

3.4 Bloco D – Contrato e resposta a problemas

Q11 Contrato de tratamento de dados e encarregado

Vocês assinam contrato ou anexo específico de tratamento de dados pessoais (papel de operador, finalidades, subprocessadores, auditoria, término)? Quem é o encarregado de dados (DPO) e como contatá-lo?

POR QUE PERGUNTAMOS

A LGPD atribui responsabilidade ao controlador e ao operador e exige que o operador trate dados conforme as instruções do controlador ([art. 39](#)); a Resolução CFM remete à proteção geral de dados ([art. 16](#)).

RESPOSTA ACEITÁVEL

Minuta de contrato de tratamento de dados disponível, nome e contato do encarregado.

Q12 Canal de falhas e prazo de comunicação de incidente

Qual é o canal para relatar falhas, erros clínicos relevantes e usos inadequados do sistema? Em quanto tempo vocês comunicam ao serviço um incidente de segurança que afete dados dos nossos pacientes?

POR QUE PERGUNTAMOS

O médico deve “comunicar (...) falhas, riscos ou usos inadequados” ([art. 7º, §2º](#)) – para isso precisa de canal. Na LGPD, o controlador comunica incidente relevante à ANPD e aos titulares ([art. 48](#)); a Resolução CD/ANPD nº 15/2024 fixa o prazo de três dias úteis para a comunicação à ANPD, o que só é viável se o operador avisar antes.

RESPOSTA ACEITÁVEL

Canal nomeado (e-mail, portal, telefone) com prazo de resposta; compromisso contratual de comunicar incidentes em prazo curto e definido, de modo que o serviço consiga cumprir os três dias úteis.

4. Ficha de avaliação

Sistema / versão

Fornecedor

Data da resposta

Nº	Pergunta	Atende	Parcial	Não	Sem resposta	Observação
Q1	Nível de risco	☐	☐	☐	☐	
Q2	Validação e situação regulatória	☐	☐	☐	☐	
Q3	Limitações e vieses	☐	☐	☐	☐	
Q4	Dados: local e subprocessadores BLOQUEANTE	☐	☐	☐	☐	
Q5	Uso para treino / opt-out BLOQUEANTE	☐	☐	☐	☐	
Q6	Retenção e descarte	☐	☐	☐	☐	
Q7	Segurança e incidentes BLOQUEANTE	☐	☐	☐	☐	
Q8	Ação sem revisão humana BLOQUEANTE	☐	☐	☐	☐	
Q9	Explicação e discordância	☐	☐	☐	☐	
Q10	Parametrização e logs	☐	☐	☐	☐	
Q11	Contrato de dados e encarregado	☐	☐	☐	☐	
Q12	Canal de falhas e prazo	☐	☐	☐	☐	

Veredito☐ Aprovado☐ Aprovado com condições☐ Reprovado

Condições ou pendências (com prazo)

Nível de risco atribuído pelo serviço (documento 1)

Próxima reavaliação (sugestão: 12 meses)

Responsável técnico — nome e CRM/UF

Data

5. Sinais de alerta

Respostas que, isoladamente, não reprovam, mas que juntas pedem cautela (*prática recomendada — não é exigência literal*):

- “Não há limitações conhecidas”, “o sistema é 100% preciso” ou qualquer promessa de resultado.
- Não sabe dizer em que país os dados ficam, ou muda a resposta entre o comercial e o técnico.
- Trata a pergunta sobre a ANVISA como irrelevante sem explicar por quê.
- Usa os dados para treinar “de forma anonimizada”, sem descrever como anonimiza nem quem verifica.
- Não tem encarregado de dados nem minuta de contrato de tratamento, mas “pode providenciar”.
- Nunca teve incidente de segurança e não tem processo para o dia em que tiver.
- A funcionalidade que age sem revisão humana “é o diferencial do produto”.
- Responde ao questionário com o material de marketing.

6. Os outros documentos do kit

Nº	Documento	Para que serve
1	Mapa de risco	Classifica cada uso de IA do serviço nos níveis do Anexo II e registra a avaliação preliminar (art. 12 e 13).
2	Registro no prontuário	Como anotar o apoio de IA no prontuário (art. 4º, V), com modelos por cenário e o que não registrar.
3	Termo de ciência	Informa o paciente sobre o uso de IA e registra sua ciência ou recusa (art. 5º, §1º e §3º; art. 10; art. 11).
4	Questionário do fornecedor (este)	Doze perguntas com dispositivo e resposta aceitável, para antes de contratar e para reavaliar (art. 3º, 6º, 13, 16 e 17).
5	Política de uso de IA	Organiza os processos internos de governança que o art. 14 e o Anexo III pedem, no tamanho de um pequeno serviço.
6	Revisão trimestral	Roteiro de 60 minutos e ficha para o monitoramento regular (art. 9º, §2º; Anexo II, §1º e §2º).
7	Prompts com a fronteira embutida	Dez prompts com o que não colar, a instrução de parada e a linha de registro — e os usos que ficaram de fora.

Referências normativas

Norma	Dados verificados
Resolução CFM nº 2.454, de 11/02/2026	Normatiza o uso da inteligência artificial na medicina. DOU de 27/02/2026 (Ed. 39, Seção 1, p. 158); retificação do art. 16 no DOU de 05/03/2026 (Ed. 43, Seção 1, p. 91). Em vigor desde 26/08/2026 (art. 23: 180 dias após a publicação). Texto integral: sistemas.cfm.org.br/normas/arquivos/resolucoes/BR/2026/2454_2026.pdf — verificado em 2026-08-30.
Resolução CFM nº 2.217, de 27/09/2018	Código de Ética Médica. DOU de 01/11/2018, Seção 1, p. 179. portal.cfm.org.br/images/PDF/cem2019.pdf
Resolução CFM nº 2.314, de 20/04/2022	Define e regulamenta a telemedicina. sistemas.cfm.org.br/normas/arquivos/resolucoes/BR/2022/2314_2022.pdf
Lei nº 13.709, de 14/08/2018 (LGPD)	Lei Geral de Proteção de Dados Pessoais. planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
Resolução CD/ANPD nº 15, de 24/04/2024	Regulamento de Comunicação de Incidente de Segurança. Publicada no DOU (in.gov.br).

A numeração dos artigos citada neste kit foi conferida contra o PDF oficial da Resolução CFM nº 2.454/2026. Antes de citar em documento próprio, confira a versão vigente no site do CFM.

Sobre o autor

Carlos Avila é médico e atua em informática em saúde e proteção de dados. Escreve na saude.dev sobre software clínico, LGPD e as normas do CFM que alcançam a tecnologia usada por médicos e serviços de saúde. Ecossistema: higeia.io · anot.ae · capacita.ai

Licença **Creative Commons Atribuição 4.0 Internacional (CC BY 4.0)**. Você pode copiar, saude.dev/kits/ia-no-consultorio adaptar e redistribuir este documento, inclusive para uso comercial, desde que mantenha a atribuição “saude.dev / Carlos Avila” e indique as alterações feitas.