

Proposta de Padrão Aberto para Interoperabilidade de Governança de IA em Saúde no Brasil

Entidade proponente: ArkMED

Proposta pública para discussão multissetorial

Versão 0.2 • 28 de outubro de 2026

Proposta de um contrato aberto de dados e interfaces para identificar soluções, compartilhar evidências, acompanhar mudanças e apoiar decisões responsáveis sobre IA em saúde.

Situação do documento. Esta é uma proposta pública apresentada pelo ArkMED para discussão e construção multissetorial. Não constitui norma oficial, certificação, parecer jurídico, anuência de autoridade ou comprovação de conformidade de qualquer produto. Os verbos DEVE, DEVERIA e PODE descrevem requisitos propostos do padrão, conforme a seção 3.

Recorte da pesquisa. Fontes consultadas em 28/10/2026. A análise distingue instrumentos brasileiros vigentes, referências internacionais, documentos em desenvolvimento e sugestões para adoção futura. Os exemplos são fictícios; não representam produtos, estudos, pessoas ou autorizações reais.

Preparação e revisão. Documento elaborado com assistência de IA, pesquisa em fontes primárias e consulta a materiais internos de projetos em desenvolvimento da entidade proponente, identificados nas referências. A aprovação institucional, a revisão jurídica especializada e a validação técnica pelas partes interessadas permanecem etapas de uma futura consulta. Nenhuma consulta externa ou submissão foi realizada nesta tarefa.

1. Síntese executiva

Instituições de saúde precisam saber qual solução de IA utilizam, em qual versão, para qual finalidade, com quais limitações e evidências. Essas informações costumam estar distribuídas entre contratos, instruções de uso, publicações, portais e comunicações do fornecedor. Mudanças em modelos, dependências e condições de uso dificultam a manutenção de um inventário confiável e de decisões institucionais rastreáveis.

Propõe-se um **Padrão Aberto de Interoperabilidade de Governança de IA em Saúde**, designado neste documento pela sigla de trabalho **PAIG-IA Saúde**. O nome é provisório, sem pretensão de reconhecimento oficial. O padrão seria um contrato de dados legíveis por máquina, acompanhado de regras de publicação, autenticidade, atualização, acesso e avaliação contextual. Uma API é um meio de implementação; um arquivo JSON assinado também pode atender ao nível inicial.

O núcleo contém quatro objetos: **produto**, **release**, **afirmação com evidência** e **evento de mudança**. Um quinto objeto, a **implantação institucional**, pertence à instituição e relaciona a configuração efetivamente usada às avaliações e decisões locais. A rastreabilidade segue: organização → produto → release → componentes → implantação → decisão → evidências.

Para desenvolvedores e fornecedores de IA, um contrato comum permite reutilizar informações de governança em múltiplas integrações, reduzindo adaptações específicas por contratante. **Para desenvolvedores de catálogos, auditoria e governança**, interfaces abertas criam condições para implementar serviços compatíveis e competir pela qualidade, com portabilidade de dados.

Para instituições de saúde, o padrão pode facilitar a comparação de evidências, o acompanhamento de alterações e a manutenção de inventários e decisões documentadas. Cada instituição poderá integrar os dados aos sistemas que escolher. Esses benefícios dependem de adesão, qualidade das informações e validação nos pilotos.

Decisão central. Recomenda-se começar com publicação voluntária, pilotos entre fornecedores e instituições e testes de portabilidade. Uma eventual obrigação regulatória dependerá de instrumento próprio, competência legal, avaliação de impacto e consulta pública. A pesquisa não identificou nas normas examinadas obrigação geral de todo fabricante de IA em saúde oferecer uma API de governança.

Resultado esperado. Reduzir o retrabalho de coleta e tornar mudanças detectáveis, sem automatizar decisões clínicas, substituir a avaliação institucional ou confundir informação declarada com verificação independente.

Guia de leitura

As seções 2-5 delimitam o contexto jurídico e internacional; 6-8 tratam de governança, arquitetura e identidade; 9-17 especificam dados, evidências, acesso, segurança, comunicação e avaliação; 18-20 apresentam adoção, redação institucional sugerida e limites; os anexos trazem payloads fictícios e referências verificáveis.

2. Escopo e enquadramento jurídico

2.1 Objetivo e fronteiras

O padrão cobre IA clínica, administrativa, de pesquisa e de uso geral empregada em saúde, com perfis proporcionais à finalidade e ao risco. O escopo informacional é mais amplo que o de software como dispositivo médico. Estar no catálogo não equivale a regularização sanitária; aderir ao padrão não autoriza uso assistencial.

Ficam fora do núcleo: trânsito de prontuários, inferência clínica, entrega de pesos de modelos, compartilhamento indiscriminado de bases de treinamento e emissão automática de certificados legais. Evidências detalhadas podem ser disponibilizadas por canal controlado, quando cabível. O núcleo não cria nova hipótese legal para tratamento de dados.

2.2 Quadro de situação em 28/10/2026

Instrumento	Situação e alcance relevante	Consequência para a proposta
Resolução CFM nº 2.454/2026	Em vigor; uso e governança de IA na medicina. Publicada em 27/02/2026, retificada em 05/03/2026; vigência informada pelo CFM em 26/08/2026 [01-02].	Mapear deveres profissionais e institucionais, sem atribuir ao CFM uma homologação geral de fornecedores.
RDC Anvisa nº 657/2022	Regularização de SaMD; vigente na base temática consultada [03].	Registrar enquadramento e finalidade, inclusive exclusões e condições de exceção.
RDC Anvisa nº 751/2022	Classificação e regimes de notificação e registro de dispositivos médicos, com alterações [04].	Distinguir classe sanitária, regime e situação; não reproduzir classificações antigas de manuais.
LGPD e regulamentação ANPD	Deveres sobre tratamento de dados e instrumentos específicos [05-08].	Minimizar dados, controlar acessos e tratar incidentes e transferências de forma adequada.
PL nº 2.338/2023	Na Câmara, aguardando parecer na Comissão Especial na consulta realizada [09].	Tratar como projeto legislativo, sem converter seu conteúdo em obrigação vigente.
PAIG-IA Saúde	Proposta apresentada neste documento.	Adesão inicialmente voluntária ou contratual; eventual incorporação oficial exige processo próprio.

2.3 Três sentidos que devem permanecer separados

Regularização sanitária é a situação perante a Anvisa, quando aplicável. **Habilitação ou aprovação institucional** é a decisão documentada da instituição para um uso específico. **Conformidade com o padrão** é o atendimento a um perfil técnico de intercâmbio de dados. Evita-se usar “homologado no Brasil” sem indicar autoridade, ato, objeto, condições e prazo.

3. Fundamentos brasileiros e linguagem de requisitos

3.1 CFM: fundamento para interoperabilidade

A Resolução CFM nº 2.454/2026 estabelece governança no art. 14; seu parágrafo único prevê Comissão de IA e Telemedicina para instituições que adotem sistemas próprios. O Anexo III, itens IV e VII, trata de padrões abertos, APIs e integração; o item VI aborda o ciclo de vida. Isso apoia a iniciativa, mas não institui uma API universal de fabricantes. A norma também preserva supervisão e autonomia médicas [01].

Aplicação proposta: as instituições podem usar os objetos do padrão para reunir informações e evidências dos seus processos. A composição de comitês, as responsabilidades e a avaliação de cada uso devem respeitar a norma aplicável. Os sistemas de apoio à governança não assumem a atribuição do diretor técnico nem a competência fiscalizatória dos Conselhos.

3.2 Anvisa: finalidade, versão e regularização

A RDC nº 657/2022 disciplina SaMD e possui exclusões e tratamento específico para desenvolvimento interno, sob condições. A RDC nº 751/2022 distingue notificação, para classes I e II, e registro, para III e IV; sua Regra 11 disciplina software. O enquadramento depende da finalidade e das regras aplicáveis, não apenas da presença de IA [03-04].

A RDC nº 657/2022 também trata da coerência entre produto e informações de regularização e do acompanhamento pós-mercado pelos canais oficiais. A manutenção de metadados no padrão não substitui peticionamento, tecnovigilância ou ação de campo [03].

Aplicação proposta: guardar a referência do ato, a finalidade e os identificadores relevantes; consultar a fonte oficial e registrar a data da consulta. Situações como “não se enquadra”, “dispensado sob condições” e “em análise” exigem racional identificado. Um protocolo de solicitação não deve ser apresentado como deferimento. Regras de IVD e de software embarcado demandam enquadramento específico; não se aplica automaticamente o mesmo caminho a todo software de saúde.

3.3 Como ler DEVE, DEVERIA e PODE

DEVE indica condição de conformidade com o perfil técnico proposto. **DEVERIA** indica recomendação que admite desvio documentado. **PODE** indica opção. Essas palavras não transformam o documento em lei. Prazos e métricas identificados como “meta do piloto” ou “propostos” não são prazos regulatórios.

Cada regra regulatória modelada em um consumidor DEVE ter jurisdição, instrumento, dispositivo, versão do texto, datas de aplicação e revisão humana. Uma revisão normativa pode alterar a avaliação sem que o produto tenha mudado. A relação entre controles e normas é uma ajuda à análise, nunca prova suficiente de cumprimento.

4. Proteção de dados: LGPD e ANPD

4.1 Base jurídica verificada

A LGPD considera dados de saúde sensíveis. O tratamento exige hipótese adequada, observância dos princípios e medidas de segurança. Legítimo interesse não integra as hipóteses do art. 11 para dados sensíveis. O art. 20 prevê revisão de decisões exclusivamente automatizadas que afetem interesses, sem impor em sua redação atual uma revisão necessariamente por pessoa natural. O RIPD pode ser exigido pela ANPD; não é obrigação indistinta para todo uso de IA [05].

A Resolução CD/ANPD nº 15/2024 disciplina comunicação de incidentes com risco ou dano relevante: em regra, três dias úteis para comunicação pelo controlador à ANPD e aos titulares, com marco de conhecimento e ressalvas normativas; há tratamento diferenciado para pequenos agentes elegíveis [06]. A Resolução nº 19/2024, com retificação de 2025, rege transferências internacionais. A Resolução nº 32/2026 reconhece adequação da União Europeia no âmbito previsto [07-08].

4.2 Requisitos de projeto propostos

Separação de ambientes. O manifesto público DEVE conter metadados de governança, sem dados de pacientes, exemplos clínicos identificáveis ou prompts de produção. O ambiente de evidências restritas DEVE ter controle de acesso e retenção definidos. Logs de integração não devem capturar tokens, prontuários ou conteúdo de inferências.

Responsabilidades documentadas. Cada fluxo DEVE identificar suas finalidades, controlador, operador quando houver, suboperadores, categorias de dados, localização de processamento e canal do encarregado. A qualificação depende das atividades efetivas; o contrato, isoladamente, não decide os papéis. Operadores de catálogos, plataformas de governança, fornecedores e instituições podem ter papéis diferentes conforme o fluxo.

Avaliação antes do envio. A instituição DEVE verificar necessidade, base jurídica, sigilo profissional, direitos dos titulares e condições de transferência antes de carregar uma evidência. Consentimento assistencial, consentimento para pesquisa e base jurídica de proteção de dados são análises distintas. Pseudonimização não significa anonimização; resultados agregados também podem permitir reidentificação.

Transferências. Registrar país, destinatário, finalidade, mecanismo utilizado e transferências subsequentes. A adequação de um destino não elimina os demais deveres. A infraestrutura não DEVE afirmar que toda hospedagem fora do Brasil é proibida ou que cláusulas-padrão são sempre o único mecanismo possível.

Gestão de incidentes. O evento técnico do padrão DEVE alimentar a triagem jurídica e de segurança, sem esperar a conclusão editorial de uma ficha. Webhooks não substituem os canais oficiais. Prazos contratuais precisam permitir que o controlador cumpra seus prazos legais.

5. Referências internacionais e reaproveitamento

5.1 AI Act: referência, alcance e calendário

O Regulamento (UE) 2024/1689 adota requisitos de documentação, registros, transparência, supervisão e acompanhamento conforme o enquadramento. Sua aplicação territorial deve ser examinada para cada atividade; ele não se converte em lei brasileira por ser citado. Também não cria uma API universal de governança [10].

O calendário original não deve ser repetido sem atualização. A Comissão Europeia informa que o AI Omnibus entrou em vigor em 27/07/2026: regras de alto risco do Anexo III passaram a ter aplicação em 02/12/2027, e as correspondentes a produtos regulados do Anexo I, em 02/08/2028. A fonte institucional identifica a alteração como Regulamento (UE) 2026/1744 [11]. Para casos concretos, verificar o texto consolidado, o enquadramento e as disposições transitórias pertinentes.

5.2 Mapa de compatibilidade proposto

Referência	Reaproveitamento recomendado	Limite a preservar
CycloneDX 1.7 / ECMA-424, 2ª ed., 2025 [12-13]	AI/ML-BOM, componentes, dependências, model cards, referências e declarações.	Um inventário de componentes não é avaliação clínica nem autorização sanitária.
Model Cards for Model Reporting, 2019 [14]	Finalidade, populações avaliadas, desempenho e limitações.	Model card é documentação; o nível de verificação precisa ser informado.
HL7 FHIR R4, Provenance [15]	Relacionar autoria e transformação de recursos clínicos à identidade da solução.	FHIR não substitui o catálogo de governança nem determina adequação do uso.
HL7 AI Transparency on FHIR, 1.0.0-ballot [16-17]	Identificação de participação da IA e proveniência ligada a model card.	Edição consultada é ballot/STU em desenvolvimento; fixar versão e testar o perfil.
NIST AI RMF 1.0, 2023 [18]	Organizar atividades de governança e gestão de riscos.	Referência voluntária e não setorial; não equivale a certificação.
OMS, Regulatory considerations on AI for health, 2023 [19]	Transparência, documentação e avaliação ao longo do ciclo de vida.	Orientação internacional, sem força normativa brasileira automática.

A estratégia é criar um **perfil brasileiro de ligação**, evitando duplicar estruturas existentes. Cada adaptador DEVE declarar versão de origem, versão de destino, transformações e perdas. Não se declara equivalência integral entre padrões com escopos distintos.

6. Governança institucional do padrão aberto

6.1 Estrutura proposta

Sugere-se constituir um fórum multissetorial com representantes de instituições públicas e privadas, desenvolvedores, profissionais de saúde, pacientes, academia, especialistas em proteção de dados e entidades de interoperabilidade. Autoridades podem ser convidadas, sem presumir participação, apoio ou delegação. O ArkMED é a entidade proponente desta iniciativa. O arranjo de manutenção do padrão deverá ser definido de forma multissetorial, com responsabilidades transparentes e participação aberta a outras organizações.

Um **conselho de governança** aprovaria políticas e versões; um **comitê técnico** manteria esquema, vocabulários e testes; uma **câmara clínica e ética** revisaria cenários e impactos; e uma **secretaria** administraria consultas, registro de decisões e suporte. Os papéis podem ser acumulados no piloto, com conflitos declarados e separação entre avaliação e interesse comercial.

6.2 Processo decisório e independência

As propostas de alteração DEVEM ser públicas, numeradas e acompanhadas de justificativa, exemplos, impacto de compatibilidade e plano de migração. Propõem-se consulta de pelo menos 45 dias para versões estáveis e decisão por consenso; na falta dele, voto de dois terços com representação de ao menos três grupos de interesse. Esses parâmetros são sugestões de estatuto, não regras já instituídas.

Fabricantes ou financiadores não DEVERIAM controlar a maioria dos votos. Conflitos, patrocínios e abstenções DEVEM ser publicados. O processo DEVE oferecer contestação de decisões, correção de dados e recurso a revisores sem conflito. Uma contestação não deve apagar o registro histórico do fato contestado.

6.3 Abertura, licenças e sustentabilidade

Recomenda-se especificação e vocabulários sob licença aberta compatível com ampla reutilização, e ferramentas de referência sob licença permissiva, após revisão de direitos. É uma política proposta; este documento não concede licenças de materiais de terceiros. O acesso às especificações e aos testes essenciais não DEVE depender da contratação de qualquer fornecedor específico.

Dados e evidências mantêm licenças e restrições próprias. Uma licença de código não autoriza redistribuir artigos, documentos confidenciais ou dados pessoais. Deve existir exportação integral dos dados próprios do participante em formato aberto, sem retenção contratual que impeça a migração.

6.4 Confiança e correções

O fórum DEVE publicar versões, atas, alterações, política de segurança e critérios de conformidade. Uma lista de implementadores DEVE informar perfil, versão, data e escopo do teste. É vedado usar o selo do padrão para sugerir aprovação clínica ou regulatória. Custos podem ser cobertos por contribuições, suporte e serviços de validação, preservando acesso público ao núcleo.

7. Arquitetura federada e possibilidades de implementação

7.1 Fluxo de referência

Fornecedor → **publicador assinado** → **consumidores autorizados** → **avaliação local** → **decisão humana e monitoramento**. Catálogos e sistemas institucionais podem consumir os dados. A instituição também pode integrar-se diretamente ao publicador, sem intermediação obrigatória de registro ou plataforma. Os dados clínicos permanecem em seu ambiente próprio.

Fornecedor	Publica produto, releases, evidências e alertas
Publicador	Arquivo HTTPS ou API; documentos assinados
Catálogos / redes	Organizam informações, fontes e histórico
Instituições	Sistemas próprios ou contratados apoiam a avaliação local

Um fornecedor PODE operar seu publicador ou delegá-lo a prestador autorizado. Espelhos DEVEM preservar o documento original, a assinatura e a identidade do emissor. Descoberta, exportação e resolução de identidade devem permitir a continuidade quando um agregador estiver indisponível.

7.2 Integrações abertas a diferentes participantes

Desenvolvedores independentes podem implementar publicadores, conectores, catálogos e ferramentas de auditoria ou governança. Hospitais, clínicas, redes e serviços públicos podem integrar as informações aos sistemas próprios ou contratados. O mesmo formato deve atender a múltiplos consumidores, preservando permissões, licenças e proveniência.

Uma declaração do fabricante permanece identificada como tal. Verificações de fontes e avaliações institucionais são objetos separados, com autor, escopo e data. Receber um evento pode iniciar uma reavaliação; não aprova automaticamente uma atualização. Esses princípios se aplicam a qualquer implementação.

7.3 Projetos em desenvolvimento do proponente

O ArkMED desenvolve dois projetos: o **ReBIAM (Registro Brasileiro de IA em Medicina)**, voltado a um catálogo público e rastreável de soluções de IA em medicina, com fontes por informação [I1-I2]; e o **GovIA**, voltado ao apoio à governança institucional de IA, incluindo inventário, riscos, avaliações de impacto, responsabilidades e evidências [I3]. **Ambos são projetos em desenvolvimento.**

Como exemplos de aplicação futura, o ReBIAM poderá consumir informações públicas, e o GovIA poderá apoiar avaliações locais com dados autorizados. Essas possibilidades dependem de desenvolvimento e validação. O padrão admite implementações por quaisquer organizações, com os mesmos critérios de participação e conformidade técnica.

8. Identidade, releases e versionamento

8.1 Identificadores persistentes

Cada organização DEVE possuir identificador estável e verificável. CNPJ e identificadores estrangeiros são atributos auxiliares, quando aplicáveis; não bastam como identificador de produto. Cada produto DEVE ter URI ou UUID persistente, sem reutilização após encerramento. Mudança de nome comercial não gera nova identidade; mudança de titularidade exige evento e vínculo histórico.

Uma release DEVE ter identificador imutável e referenciar produto, versão comercial, data de disponibilização e componentes relevantes. Um alias como latest PODE existir para descoberta, mas não DEVE ser usado isoladamente em evidências ou decisões. O registro institucional DEVE preservar o identificador resolvido e o instante da resolução.

8.2 Cinco versões diferentes

Camada	Identificação proposta	Quando mudar
Padrão	standardVersion, como 0.1.0	Alteração do contrato semântico. Durante a série 0.x, compatibilidade não é presumida.
API	Caminho de versão principal e contrato OpenAPI fixado	Alteração incompatível da interface.
Documento	documentId, revision, issuedAt, supersedes	Toda correção de conteúdo, inclusive editorial.
Produto e componentes	releaseId, softwareVersion, modelVersion, hashes	Alteração do artefato ou de dependência que afete a release.
Implantação	deploymentRevision, configuração e ambiente	Alteração local, incluindo limiar, prompt, base RAG ou integração.

Versão semântica PODE ser usada pelo fornecedor; não DEVE ser inferida a partir de um rótulo comercial. A relevância clínica da mudança não pode ser deduzida de ser uma versão “minor” ou “patch”.

Risco em eixos distintos. Classificação sanitária, classificação nos termos do CFM e avaliação institucional DEVEM ser objetos separados. Cada um registra esquema e versão, classe, avaliador, data, fundamento e contexto. Não se converte automaticamente classe Anvisa em categoria CFM ou resultado local.

8.3 IA composta, serviços e modelos generativos

A identidade da solução DEVE incluir, conforme aplicável: modelo base e revisão, ajuste fino, políticas de sistema, templates de prompt, ferramentas autorizadas, índice/base RAG, pré e pós-processamento, limiares, guardrails e versão do aplicativo. Artefatos restritos podem ser representados por identificador e compromisso criptográfico, sem divulgação do conteúdo.

Em SaaS, o fornecedor DEVE oferecer identificador da execução ou da release resolvida e período de uso; o consumidor registra observedAt e o método de observação. Se só houver alias mutável ou versão desconhecida, isso DEVE aparecer como lacuna, com limites de rastreabilidade e controles compensatórios. Aprendizado contínuo requer política de mudanças, snapshots identificáveis e avaliação; não autoriza alteração clínica silenciosa.

9. Informações mínimas: contrato de dados

As cardinalidades abaixo são requisitos propostos. **R** significa requerido; **C**, condicional; **O**, opcional. Um campo requerido pode admitir estado de desconhecimento explicitamente previsto; isso permite intercâmbio, mas não implica suficiência de evidência. Condições e enumerações precisam constar no futuro esquema normativo.

9.1 Núcleo público de produto e release

Grupo / campos	Regra	Conteúdo e validação
Envelope	R	documentId, documentType, standardVersion, profile, revision, issuedAt, validUntil, publisherId, accessLevel. Datas com fuso; revisão positiva.
Organização	R	Identificador, nome legal, país, contato institucional e relação com o produto. CNPJ, representante e detentor no Brasil quando aplicáveis.
Produto	R	productId, nome, descrição em pt-BR, categoria e URL canônica. Não usar nome como chave.
Finalidade	R	Uso pretendido, usuários, população-alvo, entradas, saídas, ambiente e exclusões de uso; intendedUseId versionado.
Release	R	releaseId, softwareVersion, status, data e vínculo ao produto; modelos/componentes identificados ou lacuna explícita.
Supervisão	R	Papel do humano, competências necessárias, revisão de saída, meios de interromper ou recusar resultado.
Limitações	R	Contraindicações, incompatibilidades e falhas conhecidas, ou justificativa documentada de avaliação ainda incompleta.
Regulação	R/C	Objeto de situação com jurisdição, enquadramento e origem; número, regime e ato quando aplicáveis; fonte e consulta.
Evidências	R	Lista de referências e afirmações vinculadas, ou estado explícito de indisponibilidade. Lista vazia não significa validação satisfatória.
Ciclo de vida	R	Política e canal de avisos, suporte, fim de vida, histórico e data prevista de revisão.
Autenticidade	R	Assinatura externa verificável do documento, referência de chave e política de confiança; hash nos artefatos referenciados.

9.2 Estados de ausência

Usar objetos com status, como known, unknown, not_assessed, not_applicable e withheld. Quando não houver valor, registrar reason, responsável e data; para not_applicable, incluir racional de enquadramento; para withheld, classificação e caminho de acesso autorizado. Não usar texto vazio, zero ou false para representar desconhecimento.

O consumidor DEVE distinguir ausência de informação, negativa de acesso e inexistência de requisito. Campos condicionais não podem ser contornados com “não se aplica” sem justificativa. Identificadores de normas e vocabulários DEVEM possuir namespace e versão.

10. Extensões de evidência, dados e operação

10.1 Informações para análise institucional

Grupo	Conteúdo mínimo quando aplicável
Validação	Desenho, objetivo, datas, versão avaliada, população, centros, país, inclusão/exclusão, tamanho e unidade de análise. Distinguir pacientes, exames e registros.
Desempenho	Métrica, definição, estimativa, intervalo de confiança e método, denominador, limiar, referência de verdade e cenário de aplicação.
Generalização e equidade	Validação externa, independência dos conjuntos, subgrupos relevantes, tamanhos, incerteza e grupos não avaliados. Ausência de diferença observada não prova ausência de viés.
Dados e treinamento	Proveniência e categorias, períodos, geografia, licenças/direitos e governança; descrição proporcional sem obrigar divulgação de dados individuais ou segredos.
Privacidade	Finalidades, categorias de dados, retenção, localização, suboperadores, transferências, canal de direitos e política de uso de dados para treinamento.
Segurança	Política de vulnerabilidades, canal de reporte, suporte, dependências/BOM, controles e avisos pertinentes; detalhes exploráveis sob acesso restrito.
Monitoramento	Indicadores, linha de base, critérios de deriva, limiares de ação, periodicidade e responsáveis; desempenho em produção separado de estudo original.
Implantação	Unidade, serviço, finalidade local, release observada, configuração, dependências locais, responsável e decisão de uso com condições.

10.2 Qualidade semântica

Cada métrica DEVE apontar para um estudo e uma versão específica. Uma AUROC não substitui sensibilidade, especificidade, calibração, valores preditivos ou avaliação de utilidade clínica. Métricas pertinentes dependem do problema. Valores preditivos e desempenho podem mudar com prevalência, equipamentos e fluxo de trabalho; comparar números exige contexto compatível.

Para IA generativa, DEVERIAM ser documentados: protocolo e conjuntos de avaliação, erros factuais, omissões, fidelidade à fonte, comportamento diante de solicitações inadequadas, privacidade, segurança de ferramentas e avaliação humana. Uma pontuação genérica de benchmark não autoriza uso clínico. A aplicabilidade do protocolo ao português brasileiro e ao contexto assistencial precisa ser explicitada.

10.3 Vocabulários e extensões

Textos destinados a usuários brasileiros DEVEM oferecer pt-BR nos campos essenciais. Vocabulários reutilizáveis devem ter identificadores estáveis e licença adequada. Códigos clínicos ou terminologias podem ser referenciados quando úteis e licenciados, sem impor um único sistema a todos os campos.

Extensões DEVEM possuir namespace, versão e definição pública de semântica. Consumidores podem ignorar extensões opcionais, mas DEVEM rejeitar ou encaminhar para revisão uma extensão declarada como crítica que não compreendam. Isso evita que um campo novo de segurança seja silenciosamente descartado.

11. Afirmações, evidências e verificação

11.1 Estrutura de uma afirmação

Uma *claim* DEVE identificar emissor, sujeito, release, contexto, conteúdo da afirmação, data e evidências. Cada evidência DEVE registrar título, tipo, autor/entidade, data, versão do artefato, URL ou localização controlada, hash quando houver cópia, licença e nível de acesso. Links externos mutáveis exigem data de acesso e, quando legalmente possível, preservação da cópia examinada.

A proveniência DEVE ser por afirmação ou campo, e não apenas por ficha. Uma publicação científica pode sustentar uma métrica, mas não necessariamente a situação regulatória. Um ato sanitário pode sustentar uma regularização, sem validar todas as alegações comerciais do produto.

11.2 Estados de verificação separados

Estado	Significado operacional proposto
Declarado	Conteúdo fornecido pelo emissor, sem confirmação independente.
Integridade verificada	Hash e assinatura conferidos; identidade da chave validada conforme política. Não verifica a veracidade clínica.
Fonte conferida	Revisor confirmou que a referência contém o dado declarado; não implica auditoria completa.
Avaliado independentemente	Entidade identificada examinou um escopo definido, por método declarado, na data registrada.
Contestado / revogado	Há objeção ou retirada documentada; manter motivo, autor e histórico.
Desatualizado	Prazo de revisão vencido ou fonte substituída, sem extrapolar conclusão para o produto inteiro.

Um objeto *verification* separado DEVE conter verificador, método, escopo, resultado, data, validade e conflito de interesse. Revisões diferentes não sobrescrevem umas às outras. *verification=passed* sem escopo e método não é suficiente. “Informação conferida” e “produto seguro” não são equivalentes.

11.3 Evidências contraditórias ou indisponíveis

O consumidor DEVE preservar divergências entre fabricante, estudo e fonte oficial, exibindo o estado de apuração. Uma afirmação não verificada pode ser intercambiada com sinalização, mas não deve receber selo de validação. Para decisões críticas, indisponibilidade de evidência pode impedir aprovação, mesmo que o manifesto seja tecnicamente válido.

O padrão DEVERIA admitir uma relação explícita entre requisito, controle, evidência e decisão. A cobertura documental é apenas uma dimensão: também são necessários exame de adequação, efetividade e contexto. Um painel não deve calcular “100% conforme à LGPD” a partir de campos preenchidos.

12. Níveis de acesso e direitos sobre informações

12.1 Quatro compartimentos propostos

Nível	Exemplos de conteúdo	Regra de acesso
L0 - Público	Identidade, finalidade, release, limitações essenciais, resumos de evidência e referências regulatórias.	Leitura sem credencial; licença de redistribuição explícita.
L1 - Institucional	Relatórios completos licenciados, contratos, detalhes de integração e validação pertinentes à contratante.	Entidade autenticada, finalidade autorizada, prazo e vínculo contratual.
L2 - Confidencial	Auditorias detalhadas, vulnerabilidades sob embargo e elementos proprietários necessários à avaliação.	Necessidade de conhecer, aprovação e registro do acesso; acordo quando cabível.
L3 - Acesso legal específico	Elementos solicitados por autoridade competente ou compartilhados sob dever legal específico.	Verificação da competência, fundamento, escopo e canal adequado. Não é credencial genérica de regulador.

O nível de acesso DEVE estar no documento e no artefato. Pertencer a um nível não confere direito automático a todos os objetos dele. Documentos públicos e restritos DEVEM ter identificadores e assinaturas distintos, com referência entre as versões. Evita-se publicar um documento único e tentar ocultar campos no navegador.

12.2 Regras de publicação

Avisos necessários à segurança de uso e limitações relevantes não DEVERIAM ser ocultados sob rótulo genérico de segredo comercial. Quando houver necessidade legítima de sigilo, o publicador DEVE oferecer resumo público seguro e canal de análise autorizada. O fórum deve permitir contestação de classificações excessivas.

O núcleo não exige divulgar pesos, código, prompts proprietários ou bases individuais. Um hash permite relacionar versões de artefatos disponíveis para auditoria, mas não demonstra sua qualidade ou conteúdo. Até hashes e tamanhos podem revelar informações sobre documentos previsíveis; metadados sensíveis devem ficar restritos.

12.3 Direitos e proteção por padrão

O consumidor DEVE verificar autorização para copiar, armazenar e redistribuir evidências. Referenciar artigo pago não autoriza publicar seu texto. Uma pessoa revisora pode ser identificada por papel e organização na camada pública, mantendo a vinculação individual no registro protegido quando necessário.

Catálogos públicos DEVERIAM receber apenas L0; exceções exigiriam finalidade e governança próprias. Sistemas de governança institucional DEVERIAM separar instituições e permissões por objeto, impedindo que dados de uma contratante apareçam em outra. Exportação, exclusão e retenção precisam considerar direitos, deveres de guarda e preservação de evidências.

13. Autenticidade e cadeia de confiança

13.1 Perfil criptográfico inicial proposto

Recomenda-se JSON em UTF-8, canonicalização JCS conforme RFC 8785 e assinatura JWS conforme RFC 7515 [20-21]. O perfil inicial DEVE fixar uma lista de algoritmos admitidos; propõe-se ES256 como algoritmo obrigatório do piloto, sujeito à revisão técnica. O consumidor DEVE rejeitar none e qualquer algoritmo fora de sua política. Não se confunde assinatura de aplicação com modalidade jurídica de assinatura exigida em outro procedimento.

A assinatura será um **JWS compacto com payload incorporado**, mantido em arquivo ou resposta paralela ao JSON legível. O payload é a sequência exata de bytes canonicalizados do documento; o JWS não é inserido dentro do próprio objeto que assina. O cabeçalho protegido inclui alg e kid. A validação compara o conteúdo decodificado com o documento canonicalizado e confere a chave autorizada do emissor.

13.2 Vínculo entre chave e organização

O kid DEVE resolver em cadastro de confiança aprovado pelo consumidor, contendo chave pública, organização, função autorizada, período de validade e situação de revogação. Domínio HTTPS e prova de controle são úteis, mas não substituem a verificação da entidade e de sua representação. A chave indicada pelo próprio documento não é confiável só por estar ali.

URLs de chaves não podem provocar busca arbitrária sem política. O consumidor DEVE usar lista de emissores/chaves previamente aprovados ou processo controlado de cadastro. Certificados ICP-Brasil PODEM integrar um perfil futuro quando adequados, sem pressupor que toda publicação de metadados exija esse mecanismo.

13.3 Rotação, revogação e preservação

O publicador DEVE anunciar rotação, manter sobreposição controlada de chaves e publicar comprometimentos por canal independente. O consumidor DEVE diferenciar chave expirada, revogada e assinatura inválida. Revogação por comprometimento exige examinar quando os documentos foram emitidos e quais evidências temporais são confiáveis.

Datas declaradas em JSON não são carimbo do tempo confiável. Para preservação probatória, DEVERIAM ser usados registros de recebimento assinados ou mecanismos de carimbo e arquivamento compatíveis com o risco. Guardar documento, JWS, chave/cadeia aplicável, política e resultado da verificação permite reconstituir o exame.

Três perguntas diferentes: quem publicou; se o conteúdo foi alterado; se a afirmação é verdadeira e aplicável. Assinatura responde às duas primeiras dentro de uma cadeia de confiança. A terceira depende de evidências e avaliação.

14. Segurança, privacidade e resiliência

14.1 Controles mínimos propostos

Publicadores e consumidores DEVEM usar HTTPS com configuração atualizada, proteção das chaves privadas, gestão de segredos, registros de acesso, cópias de segurança e recuperação testada. A API pública deve ser predominantemente de leitura; interfaces de publicação e administração exigem autenticação forte, autorização e segregação de funções.

Para acesso restrito, propõe-se OAuth 2.0 com práticas atuais de segurança da RFC 9700 [22], credenciais de curta duração e escopos por função e organização. Integrações de serviço podem usar autenticação de cliente forte; o desenho final precisa fixar fluxos e requisitos de tokens. Validar emissor, audiência, expiração e permissões, além da assinatura do token. Não colocar credenciais em URLs.

14.2 Ameaças específicas

Ameaça	Controle proposto
Manifesto falso ou release trocada	Assinatura, emissor autorizado, IDs imutáveis, comparação de hash e registro histórico.
Replay e evento fora de ordem	Identificador único, sequência por produto, janela temporal, deduplicação e reconciliação pelo feed.
SSRF por URL de evidência ou webhook	Verificação de destinos, bloqueio de redes internas/metadados, limites de redirecionamento, timeout e tamanho.
Vazamento entre instituições	Autorização por objeto e locatário, testes de isolamento, logs e revisão de permissões.
Arquivo malicioso ou excesso de recursos	Quarentena, verificação de tipo, análise de conteúdo, limites de tamanho, profundidade e taxa.
Instruções maliciosas em textos de evidência	Tratar conteúdo externo como dado; revisão humana e isolamento de assistentes que o processem.
Dependência indisponível ou fornecedor encerrado	Exportação, espelhos autorizados, cópia assinada, plano de continuidade e contato de emergência.

14.3 Disponibilidade sem falsa garantia

O consumidor DEVE apresentar a idade da informação, a última sincronização bem-sucedida e falhas de atualização. Indisponibilidade do publicador não prova irregularidade do produto; dados vencidos também não podem parecer atuais. A decisão de continuar, restringir ou suspender o uso depende da criticidade e do plano institucional.

A retenção DEVE ser definida por tipo de documento, fundamento e finalidade, conciliando auditoria, obrigações aplicáveis e minimização. Uma proposta de feed reter 180 dias de eventos não é prazo legal de guarda. Versões necessárias para explicar uma decisão devem continuar recuperáveis conforme a política de retenção.

15. Publicação e API de referência

15.1 Contratos e formatos

O perfil inicial propõe JSON Schema 2020-12 para validação estrutural [23], com validação explícita de formatos, e OpenAPI 3.1.1 para a interface [24]. Essas versões são escolhas de compatibilidade, não afirmação de que sejam as mais recentes. Datas usam RFC 3339 com fuso; identificadores são strings opacas. O tipo de conteúdo inicial é `application/json`, sem registrar aqui um novo media type oficial.

Operação proposta	Finalidade
GET <code>/governance/index.json</code>	Descobrir produtos, perfis, documentos, assinaturas e contato. Não se reserva um caminho <code>.well-known</code> sem processo próprio.
GET <code>/v1/products/{productId}</code>	Obter identidade e finalidade do produto.
GET <code>/v1/products/{productId}/releases</code>	Listar releases, com paginação por cursor opaco.
GET <code>/v1/releases/{releaseId}</code>	Obter manifesto imutável da release e referências de revisão documental.
GET <code>/v1/documents/{documentId}/revisions/{n}</code>	Recuperar revisão exata e seu JWS por referência.
GET <code>/v1/events?cursor=...</code>	Recuperar mudanças e reconciliar notificações.
GET <code>/v1/evidence/{evidenceId}</code>	Obter evidência ou metadados, sujeito à autorização por objeto.
POST <code>/v1/subscriptions</code>	Criar assinatura de eventos, apenas no perfil correspondente e para clientes autorizados.

15.2 Comportamento interoperável

O servidor DEVE anunciar perfis e versões suportados. Listagens devem declarar ordenação e cursor; o cursor não pode expor dados internos. ETag e If-None-Match DEVERIAM apoiar sincronização; 304 só indica que a representação não mudou. Dados restritos precisam de política de cache privada e de prevenção de mistura entre usuários.

Respostas devem distinguir requisição inválida (400), falta de autenticação (401), acesso negado (403), objeto não encontrado (404), indisponibilidade (503) e limite de taxa (429, com orientação de tentativa posterior). Para impedir enumeração, uma política pode uniformizar respostas de objetos restritos. Erros DEVEM ter código estável e identificador de correlação, sem expor segredos.

No nível de arquivo, índice, manifesto e JWS são suficientes; não se exige servidor dinâmico. Um pacote offline assinado PODE ser aceito mediante procedimento de importação, data de recebimento e alerta de desatualização. A publicação em API não deve ser pré-requisito para uma pequena empresa participar do piloto.

16. Atualizações, alertas e fim de vida

16.1 Taxonomia proposta de eventos

Os tipos mínimos são `release.published`, `document.corrected`, `intended_use.changed`, `evidence.updated`, `risk.alert`, `vulnerability.disclosed`, `regulatory.status.changed`, `release.withdrawn` e `product.end_of_life`. A versão do vocabulário DEVE acompanhar a assinatura do evento. Propõe-se envelope CloudEvents 1.0, com referência à especificação 1.0.2 [25].

Cada evento DEVE conter emissor, produto, releases afetadas, instante de detecção/publicação, gravidade justificada, ação recomendada, referência do documento atualizado e indicação de necessidade de reavaliação. Severidade do evento, classe sanitária e risco contextual são conceitos distintos. Um aviso público deve permitir identificar exposição e agir sem divulgar dados pessoais ou detalhes que facilitem exploração.

16.2 Entrega e recuperação

Webhooks DEVEM usar autenticação do destino e mensagem assinada. A entrega é pelo menos uma vez: o receptor precisa deduplicar por `source` e `id`. O ACK confirma recebimento técnico, sem significar leitura clínica, correção ou aprovação. Definir timeout, retentativas com espaçamento crescente, limite de tentativas e fila de falhas.

Todo evento entregue por webhook DEVE estar recuperável por feed. Sequência monotônica por produto e cursor de reconciliação permitem identificar lacunas e reordenamento. No piloto, propõe-se retenção mínima de 180 dias no feed e consulta diária como mecanismo de segurança; para alertas críticos, canais redundantes e escalonamento humano são necessários. A periodicidade de consulta deve acompanhar o risco e o contrato.

16.3 Metas operacionais para discussão

Evento	Meta proposta para o piloto	Resposta institucional sugerida
Risco crítico conhecido	Primeiro aviso seguro em até 24 horas após triagem inicial, com atualização progressiva.	Escalonar imediatamente ao responsável; verificar exposição e considerar restrição.
Mudança material planejada	Aviso com 30 dias de antecedência quando viável; emergência justificada.	Reavaliar antes da ativação, testar e planejar reversão.
Alteração rotineira ou correção	Publicar junto da disponibilização; preservar revisão anterior.	Conciliar inventário e registrar exame de impacto.
Fim de suporte	Antecedência contratual sugerida de 180 dias.	Migrar, preservar evidências e desativar acessos.

Essas metas não autorizam adiar contenção nem substituem prazos legais, comunicação à Anvisa ou ANPD e deveres assistenciais. Mudanças materiais incluem finalidade, população, modelo, limiar, entrada, saída, dependência relevante e configuração que altere o comportamento, ainda que o número comercial da versão permaneça igual.

17. Conformidade contextual e testes do padrão

17.1 Decidir sobre um uso concreto

Uma avaliação institucional DEVE identificar release, finalidade local, população, unidade, ambiente, integrações, configuração, responsáveis, período e versão do conjunto de requisitos. O resultado deve ser expresso como **aprovado com condições**, **piloto restrito**, **pendente**, **suspenso** ou **rejeitado**, acompanhado de justificativa e próxima revisão. A aprovação de um hospital não é transferida automaticamente a outro.

O fluxo sugerido é: inventariar → confirmar finalidade e enquadramento → examinar evidências → avaliar risco, privacidade e segurança → validar o fluxo local → decidir → monitorar → reavaliar. A avaliação de impacto algorítmico e o RIPD são documentos distintos, embora possam compartilhar evidências. A necessidade e o alcance de cada um devem ser analisados conforme o caso.

Exemplo. O fornecedor publica a release 2.1 de um apoio à análise de imagem. A instituição ainda usa 2.0, com limiar e integração próprios. O consumidor registra 2.1 como disponível, verifica se o alerta atinge 2.0 e abre revisão. Só depois dos testes e da decisão competente atualiza a implantação. Receber o manifesto 2.1 não comprova que ela esteja instalada, validada ou autorizada localmente.

17.2 Perfis de conformidade técnica propostos

Perfil	Requisitos cumulativos	O que não comprova
P1 - Publicação verificável	Manifesto e índice, núcleo mínimo, assinatura, revisões e canal de atualização; arquivos HTTPS admitidos.	Efetividade clínica ou legalidade de todo uso.
P2 - Integração contínua	P1 + API, feed, paginação, reconciliação, autenticação e exportação.	Atualização automática da instalação.
P3 - Intercâmbio contextual	P2 + evidências restritas, implantação, decisão e mapeamentos testados.	Certificação geral ou endosso de autoridade.

O teste DEVE cobrir sintaxe, semântica, IDs, condições de campos, datas, assinatura válida e inválida, revogação, falta de permissão, isolamento entre instituições, reenvio/perda de eventos, exportação e compatibilidade. Dois implementadores independentes precisam trocar objetos sem campos essenciais se perderem.

O relatório DEVE identificar implementação, versão, perfil, amostra, data, casos executados e falhas. Uma ferramenta pode passar P1 e ter evidências clínicas insuficientes. O vocabulário público de conformidade deve sempre mencionar “ao perfil técnico”, evitando “IA certificada” sem base própria.

18. Adoção progressiva e plano de piloto

18.1 Fases sugeridas, contadas da aprovação de um piloto

Fase	Horizonte indicativo	Entregas e critério de passagem
Preparação	0-2 meses	Grupo multissetorial, escopo, política de conflitos, dicionário, esquema preliminar e base de teste sintética.
P1 voluntário	3-5 meses	5-10 fornecedores e 2-3 instituições convidados; arquivos assinados e dupla implementação de leitura. Adesão não presumida.
P2/P3 em piloto	6-9 meses	Feed, avisos, reconciliação e implantação; exercício de revogação, perda de eventos e exportação.
Consulta e versão estável	10-12 meses	Relatório público sem dados sensíveis, consulta, ajustes, validação independente e especificação 1.0 candidata.
Adoção institucional	Após resultados	Cláusulas de contratação proporcionais, capacitação e suporte a pequenos desenvolvedores.
Discussão regulatória	Sem data predeterminedada	Avaliação de impacto, competência, consulta e eventual instrumento oficial, se considerado adequado pelas autoridades.

Não se propõe obrigação imediata para toda IA em saúde. A adesão contratual pode começar por objetos essenciais e entrega periódica, com alternativas de arquivo e serviços de publicação. A definição de compras públicas deve respeitar o regime aplicável e evitar exigências vinculadas a marca, plataforma ou registro privado específico.

18.2 Amostra e cenários

O piloto DEVERIA incluir pelo menos uma solução clínica sujeita a regularização, uma administrativa fora desse escopo e uma aplicação generativa com dependências externas. Deve testar fornecedor pequeno, publicação delegada e solução que não consegue informar versão exata. Um cenário de pesquisa não recebe autorização assistencial por participar do piloto.

Casos obrigatórios de ensaio: mudança de modelo sem nova versão comercial; regularização contestada; chave comprometida; estudo substituído; notificação duplicada e perdida; base RAG local alterada; retirada de release; fornecedor fora do ar; evidência não autorizada; e pedido de exportação para concorrente.

18.3 Indicadores e custos

Metas propostas para ensaio controlado: preservar todos os objetos essenciais; rejeitar todas as assinaturas inválidas; receber 95% dos eventos na janela acordada e recuperar todas as lacunas pelo feed.

Comparar com a coleta manual: custo, tempo de preparação, completude, divergências e latência dos avisos. O orçamento deve prever curadoria, segurança, infraestrutura e manutenção. A expansão depende de benefício proporcional ao esforço.

19. Redação institucional sugerida

O texto abaixo é **minuta de diretriz para consulta**. Não reproduz norma vigente nem pretende fixar competência regulatória. Pode servir de ponto de partida para política institucional, termo de adesão ou discussão normativa, após adaptação jurídica.

19.1 Princípio geral

“Os responsáveis por desenvolver, fornecer ou operar soluções de inteligência artificial utilizadas em saúde deverão, no âmbito de sua responsabilidade e conforme o instrumento de adesão, manter informações estruturadas, atualizadas e verificáveis sobre identidade, finalidade, versões, limitações, evidências e alterações relevantes, em formato aberto e com acesso proporcional à natureza da informação.”

19.2 Requisitos de disponibilização

“O cumprimento poderá ocorrer por arquivo estruturado assinado ou interface interoperável, conforme o perfil definido. A especificação, os vocabulários essenciais e os critérios de validação deverão ser públicos e implementáveis por múltiplos fornecedores. Não poderá ser exigida contratação de plataforma comercial específica para atender ao formato.”

“O fornecedor deverá vincular as informações à release pertinente, identificar o emissor de cada afirmação e comunicar alterações materiais e avisos de segurança pelos canais pactuados. A instituição deverá verificar a versão e a configuração efetivamente utilizadas e documentar sua decisão de uso, condições e revisão.”

19.3 Limites e salvaguardas

“A disponibilização não substitui regularização sanitária, avaliação clínica, deveres profissionais, obrigações de proteção de dados ou comunicações oficiais. Dados pessoais, segredos legítimos e informações de segurança serão tratados conforme sua finalidade e os limites legais, preservando acesso autorizado a evidências necessárias.”

“A declaração de conformidade com o padrão deverá indicar perfil, versão, escopo e data. Não poderá ser apresentada como aprovação sanitária, garantia de segurança clínica ou autorização irrestrita de uso.”

19.4 Caminho para eventual obrigação futura

Caso o piloto demonstre utilidade, o fórum poderá encaminhar nota técnica às instâncias competentes. Para SaMD, uma discussão com a Anvisa precisaria delimitar competência, proporcionalidade, relação com os dossiês e manutenção das informações. Para governança profissional e institucional, o diálogo com Conselhos e serviços deve preservar suas atribuições. Para proteção de dados, o padrão permanece subordinado à LGPD e à regulamentação aplicável.

Antes de qualquer adoção compulsória, DEVERIAM ser examinados custo de cumprimento, barreiras à entrada, efeitos concorrenciais, capacidade de fiscalização, transição, acessibilidade e alternativas para pequenos desenvolvedores. Consulta pública ou ambiente experimental, quando cabível, não significa aprovação da proposta ou dispensa das obrigações vigentes.

20. Limitações, decisões abertas e próximos passos

20.1 Limites substantivos

O padrão organiza informações; não produz por si só evidências faltantes, evita todo viés ou assegura segurança clínica. Um dado autêntico pode estar errado, ser insuficiente ou não se aplicar ao ambiente local. Uma solução fora do escopo de regularização sanitária pode continuar sujeita a riscos e a outros deveres.

Documentação publicada não permite observar integralmente um serviço remoto. Aprendizado contínuo, fornecedores de modelos de uso geral e cadeias de dependências podem limitar reprodutibilidade. Os consumidores devem exibir essas incertezas, sem mascará-las com uma pontuação única. Uma assinatura válida também não confirma que a release implantada corresponde ao artefato declarado.

O intercâmbio pode gerar sobrecarga para pequenos fornecedores e alertas excessivos para instituições. O piloto deve medir utilidade, permitir delegação de publicação e evitar documentação repetitiva. Métricas de subgrupos com amostra insuficiente não devem ser expostas de forma que favoreça reidentificação ou conclusões estatísticas indevidas.

20.2 O que esta versão ainda não entrega

Esta minuta não contém esquema JSON normativo completo, implementação de servidor, conjunto executável de testes ou certificação. Os payloads demonstram a semântica; precisam ser transformados em esquema, exemplos positivos/negativos e contrato interoperável antes de uma versão estável. Os mapeamentos são recomendações de desenho, não equivalências homologadas.

A pesquisa utiliza fontes oficiais e primárias acessíveis na data indicada. Parte dos portais apresentou bloqueio ou indisponibilidade: para a LGPD, foi consultado o texto compilado na Presidência; para o AI Act e a alteração de 2026, foram usadas também páginas oficiais europeias. A interpretação de um caso concreto exige verificar atos posteriores e o texto consolidado aplicável. Não foi realizada auditoria jurídica exaustiva de todo o setor.

20.3 Decisões para a próxima revisão

1. Confirmar nome, mantenedor, participantes, estatuto, licenças e política de conflitos.
2. Fechar esquema mínimo, vocabulários, perfis criptográficos e regras de compatibilidade.
3. Definir cadastro de emissores confiáveis e processo de contestação, sem registro privado obrigatório.
4. Revisar o mapa normativo com especialistas em direito sanitário, ética médica e proteção de dados.
5. Selecionar pilotos voluntários, estabelecer linha de base e obter permissões específicas para as evidências.
6. Validar exportação entre implementadores, notificações, identidade da implantação e custos de operação.

Conclusão institucional. A proposta é viável como infraestrutura aberta de informação para governança. A recomendação é validá-la de forma voluntária e multissetorial, demonstrando portabilidade e utilidade antes de discutir eventual exigência oficial.

Anexo A. Manifesto de release: exemplo fictício

Exemplo reduzido, em duas páginas, de um único documento JSON. URLs em `example.org`, nomes, IDs e versões são ilustrativos. A publicação real exige completar os campos condicionais, hospedar os artefatos e gerar uma assinatura válida. O JWS é externo; não se inclui assinatura inventada.

```
{
  "standardVersion": "0.1.0",
  "profile": "P1",
  "documentType": "release-manifest",
  "documentId": "urn:uuid:5cec69e3-e38a-4a36-a1ea-7bd6220abe10",
  "revision": 1,
  "issuedAt": "2026-10-28T10:00:00-03:00",
  "validUntil": "2027-01-28T10:00:00-03:00",
  "publisherId": "https://example.org/org/fornecedor-demo",
  "accessLevel": "L0",
  "product": {
    "productId": "https://example.org/products/apoio-demo",
    "name": "Apoio Demo - produto fictício",
    "manufacturerId": "https://example.org/org/fornecedor-demo",
    "intendedUseId": "https://example.org/uses/apoio-demo/1",
    "intendedUse": {
      "language": "pt-BR",
      "purpose": "Demonstração de intercâmbio de governança",
      "users": ["equipe de avaliação do piloto"],
      "population": "dados sintéticos, sem pacientes reais",
      "setting": "ambiente de teste sem uso assistencial",
      "inputs": ["documentos sintéticos"],
      "outputs": ["resumo para teste técnico"],
      "excludedUses": ["qualquer decisão clínica real"]
    }
  },
  "release": {
    "releaseId": "https://example.org/releases/apoio-demo/2.1",
    "softwareVersion": "2.1.0",
    "releasedAt": "2026-10-28T09:00:00-03:00",
    "status": "pilot_only",
    "components": [
      {
        "componentId": "https://example.org/models/demo/1",
        "type": "machine-learning-model",
        "modelVersion": "demo-1"
      }
    ]
  }
},
```

Leitura: `releaseId` identifica o conjunto disponibilizado pelo fornecedor; `revision` identifica esta publicação documental. A próxima página continua o mesmo objeto. `validUntil` é prazo de revisão informacional proposto e não validade de regularização sanitária.

Anexo A. Continuação do manifesto

```
"regulatory": {
  "jurisdiction": "BR",
  "authority": "ANVISA",
  "assessmentStatus": "not_assessed",
  "reason": "Produto fictício de demonstração técnica",
  "officialReference": null,
  "sourceCheckedAt": null
},
"humanOversight": {
  "required": true,
  "role": "responsável pelo ensaio técnico",
  "controls": ["revisar resultados", "interromper o teste"]
},
"limitations": [
  "Sem validação clínica; não utilizar em assistência",
  "Exemplo não representa autorização ou produto real"
],
"evidenceStatus": {
  "status": "not_assessed",
  "reason": "Não há estudo clínico neste exemplo"
},
"claims": [],
"lifecycle": {
  "supportStatus": "pilot",
  "updatesUrl": "https://example.org/governance/events",
  "policyUrl": "https://example.org/governance/policy",
  "contactUrl": "https://example.org/contact"
},
"provenance": {
  "origin": "manufacturer_declaration",
  "createdBy": "https://example.org/org/fornecedor-demo",
  "verificationStatus": "declared"
}
}
```

Assinatura e descoberta. O índice público referencia o JSON acima e um arquivo .jws. O cabeçalho protegido de uma assinatura real poderá ser {"alg": "ES256", "kid": "demo-key-2026-01"}. Esse cabeçalho, isoladamente, não é assinatura nem prova de identidade. O conteúdo JSON deve ser canonicalizado e assinado conforme a seção 13.

Ausência explícita. Os valores nulos de referência oficial e consulta são acompanhados de assessmentStatus e justificativa. O exemplo não afirma dispensa sanitária: a condição real não foi avaliada. Antes de publicar um produto real, o enquadramento deve ser registrado e os campos condicionais preenchidos. Um validador técnico pode aceitar estado desconhecido e ainda assim o consumidor impedir aprovação assistencial.

Anexo B. Afirmação e evidência: exemplo fictício

O exemplo demonstra vinculação a release e contexto. Os números foram inventados para explicar o formato e não são resultado científico. Uma evidência real deverá possuir artefato, hash calculado e descrição completa do método. Esse objeto é separado do manifesto anterior.

```
{
  "claimId": "https://example.org/claims/demo-001",
  "issuerId": "https://example.org/org/fornecedor-demo",
  "subjectReleaseId": "https://example.org/releases/apoio-demo/2.1",
  "issuedAt": "2026-10-28T10:00:00-03:00",
  "claimType": "technical_test_result",
  "statement": "Resultado fictício de ensaio com dados sintéticos",
  "context": {
    "dataset": "synthetic-demo-01",
    "analysisUnit": "document",
    "sampleSize": 200,
    "clinicalApplicability": "none"
  },
  "metric": {
    "name": "proportion_accepted_by_test_review",
    "definition": "proporção aceita segundo protocolo fictício",
    "value": 0.90,
    "numerator": 180,
    "denominator": 200,
    "confidenceInterval": {
      "status": "not_assessed",
      "reason": "Exemplo didático; não é avaliação científica"
    }
  },
  "evidence": [
    {
      "evidenceId": "https://example.org/evidence/demo-001",
      "title": "Protocolo e relatório fictícios do teste",
      "type": "synthetic_test_report",
      "date": "2026-10-28",
      "accessLevel": "L1",
      "url": "https://example.org/evidence/demo-001",
      "availability": "illustration_only"
    }
  ],
  "verification": {
    "status": "declared",
    "independentVerifier": null
  }
}
```

Não usar esse objeto como demonstração de desempenho médico. Para alegação clínica, acrescentar referência de verdade, estudo, desenho, intervalo de confiança, subgrupos e limitações pertinentes. A relação claim → evidence → verification permite que outro verificador acrescente seu exame sem alterar a declaração original.

Anexo C. Evento e implantação: exemplos fictícios

Envelope ilustrativo CloudEvents. A versão do envelope é 1.0; o perfil do conteúdo é identificado por dataschema. Os documentos e hashes reais precisam ser resolvíveis e verificados. A assinatura protege a mensagem completa por mecanismo definido no perfil, não pelo simples uso de CloudEvents.

```
{
  "specversion": "1.0",
  "id": "evt-demo-00042",
  "source": "https://example.org/org/fornecedor-demo",
  "type": "org.example.paig.release.published.v1",
  "subject": "products/apoio-demo",
  "time": "2026-10-28T10:05:00-03:00",
  "datacontenttype": "application/json",
  "dataschema": "https://example.org/schemas/event/0.1.0",
  "data": {
    "sequence": 42,
    "productId": "https://example.org/products/apoio-demo",
    "releaseId": "https://example.org/releases/apoio-demo/2.1",
    "previousReleaseId": "https://example.org/releases/apoio-demo/2.0",
    "changeCategory": "model_update",
    "requiresLocalReview": true,
    "severity": "informational",
    "action": "Avaliar antes de ativar; não atualizar inventário como instalado"
  }
}
```

Objeto local reduzido, que não deve ser enviado ao catálogo público. Serve para demonstrar que release disponível e implantada podem ser diferentes.

```
{
  "deploymentId": "urn:uuid:7cc11e68-2582-4574-9145-71965e5a1c1e",
  "deploymentRevision": 3,
  "institutionId": "https://example.org/org/hospital-demo",
  "observedReleaseId": "https://example.org/releases/apoio-demo/2.0",
  "observedAt": "2026-10-28T10:10:00-03:00",
  "observationMethod": "authenticated_runtime_metadata",
  "localConfigurationId": "https://example.org/config/demo/3",
  "assessmentId": "https://example.org/assessments/demo-017",
  "decision": "restricted_pilot",
  "clinicalUseAllowed": false,
  "conditions": ["dados sintéticos", "revisar antes de migrar para 2.1"],
  "nextReviewAt": "2026-11-15T09:00:00-03:00"
}
```

Uma resposta de runtime é evidência de observação; sua confiança depende de autenticação e do método. Não garante, sozinha, que todos os componentes executados sejam aqueles declarados.

Anexo D. Mapeamentos e roteiro de avaliação

D.1 Mapeamento de integração a validar

Objeto do padrão	Integração recomendada	Regra de transformação
Identidade da release	CycloneDX metadata.component, componentes e referências [12-13]	Preservar ID externo da release e relacionar bom-ref; não supor que um ID local do BOM é global.
Modelo e dependências	Componente machine-learning-model, modelCard e relações de dependência [13]	Fixar schema 1.7, validar artefato e declarar campos que não têm equivalente.
Finalidade e limitações	Model card do fornecedor ou documento referenciado [14]	Preservar emissor, versão, idioma e contexto; não preencher lacunas por inferência.
Origem de informação clínica	FHIR R4 Provenance, referência a Device e recurso alvo [15]	Identidade da solução relacionada à release; recurso clínico permanece no ambiente autorizado.
Participação da IA	Perfil AI Transparency on FHIR, edição 1.0.0-ballot [16-17]	Pilotar marcação e proveniência conforme o guia; não criar extensões com aparência de oficiais.
Mudança de release	Envelope CloudEvents [25]	Identidade do evento não substitui identidade imutável do documento.

Este quadro é conceitual. O piloto precisa de exemplos completos, recursos FHIR válidos e testes de ida e volta. bom-ref é referência no BOM; sua promoção a identidade global precisa de mecanismo explícito. Nem toda informação institucional tem lugar adequado em FHIR ou em AI-BOM; o padrão deve ligar documentos em vez de forçar todos os objetos em uma estrutura única.

D.2 Perguntas para exame de cada solução

1. A finalidade local coincide com a finalidade declarada e com o enquadramento sanitário aplicável?
2. A release efetivamente utilizada está identificada? O método de observação é confiável?
3. As evidências se referem a essa release, população e fluxo? Quais lacunas persistem?
4. A equipe possui supervisão efetiva, treinamento e alternativa quando o sistema falha?
5. Há finalidade e base jurídica adequadas para os fluxos de dados, incluindo terceiros e transferências?
6. Os alertas chegam a um responsável, são reconciliados e geram ações documentadas?
7. A instituição consegue restringir, suspender, exportar registros e migrar de fornecedor?
8. A decisão tem responsável competente, condições, data de revisão e trilha de evidências?

Critério de suficiência: respostas documentadas sustentam uma decisão responsável, mas não criam presunção de conformidade integral. O que permanece desconhecido deve ficar visível, com responsável e tratamento definido.

Referências verificadas: Brasil

Todas as fontes eletrônicas abaixo foram consultadas em **28/10/2026**. As URLs identificam as fontes consultadas; portais podem exigir acesso interativo. As descrições são sínteses, não transcrições das normas. Verificar versões e alterações antes de aplicar a casos concretos.

[01] **Conselho Federal de Medicina. Resolução CFM nº 2.454, de 11/02/2026.** Publicação em 27/02/2026 e retificação em 05/03/2026. Texto oficial disponibilizado pelo CFM. Dispositivos relevantes: arts. 14-19 e Anexo III, especialmente IV, VI-VIII.

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

[02] **CFM. Regras sobre uso da IA na medicina entram em vigor nesta quarta-feira, 26 de agosto.** Comunicado institucional sobre a vigência em 26/08/2026.

<https://portal.cfm.org.br/noticias/regras-sobre-uso-da-ia-na-medicina-entram-em-vigor-no-dia-26-de-agosto>

[03] **Anvisa. RDC nº 657, de 24/03/2022.** Regularização de software como dispositivo médico; publicada em 30/03/2022. Consulta ao texto na base AnvisaLegis e à lista temática de normas vigentes.

https://anvisaegis.datalegis.net/action/ActionDatalegis.php?acao=abrirTextoAto&cod_menu=9431&cod_modulo=310&link=S&numeroAto=0000657&orgao=RDC%2FDC%2FANVISA%2FMS&seqAto=000&tipo=RDC&valorAno=2022

[04] **Anvisa. RDC nº 751, de 15/09/2022.** Classificação de risco, notificação, registro, rotulagem e instruções de uso. Texto com alterações na base AnvisaLegis; arts. 6-8 e Anexo I, Regra 11.

https://anvisaegis.datalegis.net/action/ActionDatalegis.php?acao=abrirTextoAto&cod_menu=1696&cod_modulo=134&numeroAto=00000751&orgao=RDC%2FDC%2FANVISA%2FMS&pesquisa=true&seqAto=000&tipo=RDC&valorAno=2022

[05] **Brasil. Lei nº 13.709, de 14/08/2018 (LGPD), texto compilado.** Presidência da República. Pontos relevantes: arts. 5º, 6º, 7º, 11, 18, 20, 33, 37-39 e 46-50.

https://www.presidencia.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709compilado.htm

[06] **ANPD. Resolução CD/ANPD nº 15, de 24/04/2024; orientação de comunicação de incidente.** A norma e sua situação constam da lista oficial de regulamentações; os procedimentos são descritos no canal institucional.

https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis

https://www.gov.br/anpd/pt-br/aceso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd

[07] **ANPD. Resolução CD/ANPD nº 19, de 23/08/2024.** Transferência internacional de dados e cláusulas-padrão contratuais; observar retificação de 18/08/2025 indicada na lista oficial.

https://www.gov.br/anpd/pt-br/aceso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-19-de-23-de-agosto-de-2024

[08] **ANPD. Resolução nº 32, de 26/01/2026; Transferência Internacional de Dados.** Reconhecimento de adequação da União Europeia e explicação institucional dos mecanismos.

<https://www.gov.br/anpd/pt-br/assuntos/assuntos-internacionais/transferencia-internacional-de-dados>

[09] **Câmara dos Deputados. PL nº 2.338/2023, ficha de tramitação.** Situação consultada em 28/10/2026: aguardando parecer na Comissão Especial; não tratado aqui como lei.

<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2487262>

Referências verificadas: internacionais e técnicas

Data de acesso de todos os itens: 28/10/2026. Versões explicitamente escolhidas neste documento não significam necessariamente a última edição de cada tecnologia.

[10] **União Europeia. Regulamento (UE) 2024/1689, de 13/06/2024 (AI Act).** Texto original, com leitura conjunta das alterações e disposições transitórias. A consulta direta no EUR-Lex apresentou verificação de navegador; a análise foi complementada com fontes institucionais europeias.

<https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

[11] **Comissão Europeia. AI Omnibus enters into force.** Publicado em 27/07/2026, atualizado em 31/07/2026; alterações do calendário e ligação ao Regulamento (UE) 2026/1744.

<https://digital-strategy.ec.europa.eu/en/news/ai-omnibus-enters-force>

<https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng>

[12] **Ecma International. ECMA-424, 2nd edition, December 2025.** Especificação CycloneDX v1.7.

<https://ecma-international.org/publications-and-standards/standards/ecma-424/>

[13] **OWASP CycloneDX. CycloneDX v1.7 JSON Reference.** Componentes, modelCard, referências e declarações; consultar o schema da edição.

<https://cyclonedx.org/docs/1.7/json/>

[14] **Mitchell, M. et al. Model Cards for Model Reporting.** FAT* 2019; versão arXiv revisada em 14/01/2019. DOI: 10.1145/3287560.3287596.

<https://arxiv.org/abs/1810.03993>

[15] **HL7 International. FHIR R4, v4.0.1: Provenance.** Versão fixada para os mapeamentos de referência.

<https://hl7.org/fhir/R4/provenance.html>

[16] **HL7 International. AI Transparency on FHIR, v1.0.0-ballot, 2026Jan.** Guia em fase ballot/STU, baseado em R4. Não descrito nesta proposta como padrão final de maturidade normativa plena.

<https://www.hl7.org/fhir/uv/aitransparency/2026Jan/index.html>

[17] **NIST. HL7 AI Transparency on Fast Healthcare Interoperability Resources (FHIR).** Descrição institucional do projeto e de seu estágio de desenvolvimento.

<https://www.nist.gov/programs-projects/hl7-ai-transparency-fast-healthcare-interoperability-resources-fhir>

[18] **NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0).** NIST AI 100-1, 26/01/2023. DOI: 10.6028/NIST.AI.100-1.

<https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10>

[19] **Organização Mundial da Saúde. Regulatory considerations on artificial intelligence for health.** 19/10/2023.

<https://www.who.int/publications/i/item/9789240078871>

Referências de implementação e materiais contextuais

Data de acesso das fontes eletrônicas e consulta dos materiais internos: 28/10/2026. As referências de implementação fundamentam escolhas propostas, não obrigações gerais já impostas aos fornecedores brasileiros.

[20] **IETF. RFC 8785: JSON Canonicalization Scheme (JCS).** Junho de 2020. Base proposta para representação determinística do JSON assinado.

<https://www.rfc-editor.org/rfc/rfc8785>

[21] **IETF. RFC 7515: JSON Web Signature (JWS).** Maio de 2015. O perfil proposto precisa restringir algoritmos e estabelecer política de confiança.

<https://www.rfc-editor.org/rfc/rfc7515>

[22] **IETF. RFC 9700: Best Current Practice for OAuth 2.0 Security.** Janeiro de 2025.

<https://www.rfc-editor.org/rfc/rfc9700>

[23] **JSON Schema. Draft 2020-12.** Referência de esquema e vocabulários de validação; formato deve ter verificação explícita no perfil de implementação.

<https://json-schema.org/draft/2020-12>

[24] **OpenAPI Initiative. OpenAPI Specification v3.1.1.** 24/10/2024. Versão selecionada por compatibilidade para um contrato de referência.

<https://spec.openapis.org/oas/v3.1.1.html>

[25] **CNCF CloudEvents. Specification v1.0.2.** Envelope aberto de eventos; a versão do atributo specversion permanece 1.0.

<https://github.com/cloudevents/spec/blob/v1.0.2/cloudevents/spec.md>

Materiais internos de projetos em desenvolvimento

[I1] **ArkMED ReBIAM. README do repositório de desenvolvimento.** Documentação interna de projeto em desenvolvimento voltado a catálogo público, gratuito e rastreável. Descreve fontes por informação, métricas vinculadas a estudos, neutralidade e ausência de ranking, score, classificação contextual e dados de pacientes. Consultada para contextualizar o exemplo da seção 7.3; sem URL pública verificada.

[I2] **ArkMED ReBIAM. Fontes e autoria nas fichas técnicas de ferramentas de IA para medicina.** Guia interno de proveniência, autoria, revisão e nível de verificação do projeto em desenvolvimento. Consultado para contextualizar o exemplo da seção 7.3; sem URL pública verificada.

[I3] **ArkMED GovIA. Apresentação do que é o ArkMED GovIA; Instruções para Execução do Projeto, versão 0.1.** Materiais internos de projeto em desenvolvimento voltado à governança institucional de IA. Descrevem objetivos de inventário, riscos, avaliações de impacto, responsabilidades, evidências e decisões com revisão humana. Consultados para contextualizar o exemplo da seção 7.3; não comprovam funcionalidades disponíveis ou operação em produção.

Registro de integridade editorial

O documento distingue fonte regulatória, referência técnica, material interno e recomendação original. Materiais internos contextualizam os projetos citados; não constituem validação externa do padrão. Não declara apoio de CFM, Anvisa, ANPD, HL7, OMS ou NIST à proposta. Nenhum payload usa número de regularização real, chave criptográfica operacional ou dado de paciente.

Encerramento da tarefa 1. Esta entrega contém apenas a proposta técnica e institucional. O artigo para o LinkedIn não faz parte deste documento.