Journal of Health Informatics

J Health Inform. 2026;18:e1871
DOI: https://doi.org/10.59681/2175-4411.v18.iEspecial.2026.1871

ARTIGO COMPLETO
CBIS 2026

Governança da interoperabilidade segura na Saúde Digital brasileira

Governance of secure interoperability in Brazilian digital health

Luiz Renato Ramos da Cruz Alves de Lima[1] ✉, Tiago Alves Schieber[1]

ORCID: 0009-0004-5137-099X · 0000-0002-4923-7047

[1] Universidade Federal de Minas Gerais, Belo Horizonte (MG), Brasil.

FICHA DO ARTIGO

TIPO
Artigo completo · CBIS 2026

IDENTIFICADOR
e1871

DOI
10.59681/2175-4411.v18.iEspecial.2026.1871

RECEBIDO
17/05/2026

APROVADO
20/07/2026

PROCESSO DE AVALIAÇÃO
Double Blind Review

EDITOR RESPONSÁVEL
Juliano de Souza Gaspar

ACESSO
Aberto, CC BY 4.0

AUTOR CORRESPONDENTE
Luiz Renato Ramos da Cruz Alves de Lima
science@luizrena.to

LICENÇA

Este é um artigo publicado em acesso aberto sob a licença Creative Commons CC BY 4.0, que permite uso, distribuição e reprodução em qualquer meio, desde que o trabalho original seja corretamente citado.

CC BY 4.0

RESUMO

Objetivo: analisar a governança da interoperabilidade segura na Saúde Digital brasileira, com foco em regulação, conformidade e cibersegurança. **Método:** estudo documental-comparativo, com análise descritiva de dados secundários da TIC Saúde 2018-2024, dados abertos da RNDS na competência 202601 e documentos institucionais nacionais e internacionais. **Resultados:** a digitalização básica chegou a 91,6% dos estabelecimentos em 2024, mas a medida sintética de prontidão para interoperabilidade segura ficou em 41,6 pontos e o descompasso entre digitalização e prontidão permaneceu elevado, sobretudo no setor público, nas UBS e no interior. A RNDS apresentou concentração funcional em vacinação, regulação assistencial e atendimento clínico. **Conclusão:** a interoperabilidade segura exige padrões técnicos articulados a governança setorial, conformidade legal, autenticação, autorização, auditoria, resposta a incidentes e apoio proporcional às instituições com menor capacidade.

Descritores: Interoperabilidade da Informação em Saúde; Segurança Computacional; Governança em Saúde.

ABSTRACT

Objective: to analyze the governance of secure interoperability in Brazilian digital health, focusing on regulation, compliance and cybersecurity. **Method:** documentary-comparative study, with descriptive analysis of secondary TIC Saúde 2018-2024 data, RNDS open data for the 202601 reference period and national and international institutional documents. **Results:** basic digitalization reached 91.6% of health facilities in 2024, but the synthetic secure interoperability readiness measure was 41.6 points and the gap between digitalization and readiness remained high, especially in public facilities, primary care units and inland services. RNDS records were functionally concentrated in vaccination, care regulation and clinical encounters. **Conclusion:** secure interoperability requires technical standards combined with sectoral governance, legal compliance, authentication, authorization, audit trails, incident response and proportional support for institutions with lower capacity.

Keywords: Health Information Interoperability; Computer Security; Health Governance.

CBIS 2026 XXI CONGRESSO BRASILEIRO DE INFORMÁTICA EM SAÚDE

Artigo apresentado no XXI Congresso Brasileiro de Informática em Saúde (CBIS 2026), realizado de 23 a 25 de setembro de 2026, em Brasília (DF), e publicado na seção CBIS 2026 do Journal of Health Informatics.

COMO CITAR ESTE ARTIGO: de Lima LRRCA, Schieber TA. Governança da interoperabilidade segura na Saúde Digital brasileira. J Health Inform 2026;18:e1871. doi: https://doi.org/10.59681/2175-4411.v18.iEspecial.2026.1871

1 INTRODUÇÃO

A Saúde Digital brasileira vem ampliando a circulação de dados clínicos, administrativos e assistenciais entre sistemas, serviços e níveis de atenção. A Rede Nacional de Dados em Saúde (RNDS), instituída no âmbito do Programa Conecte SUS, e o uso do padrão Fast Healthcare Interoperability Resources (FHIR) tornam mais concreta a possibilidade de integração nacional de informações em saúde. Essa integração, contudo, ocorre em um campo regulatório sensível: dados de saúde são dados pessoais sensíveis, protegidos pela Lei Geral de Proteção de Dados Pessoais (LGPD), e sua circulação depende de segurança, finalidade, responsabilização e capacidade institucional de controle [1-3].

Nesse contexto, cibersegurança não é apenas uma camada técnica posterior à implantação dos sistemas. Ela compõe a própria governança da interoperabilidade. Quando registros, interfaces de programação de aplicações (APIs), credenciais e fluxos nacionais passam a conectar estabelecimentos com capacidades desiguais, a proteção dos dados e a continuidade do cuidado dependem de políticas, processos, auditoria, resposta a incidentes, gestão de fornecedores e apoio aos pontos mais frágeis da rede [4,5].

A interoperabilidade segura, portanto, não se esgota na adoção de um padrão sintático ou semântico de troca de dados. Ela pressupõe uma cadeia de confiança que envolve identificação de usuários e sistemas, autorização por finalidade, proteção das bases, rastreabilidade de acessos, gestão de vulnerabilidades e capacidade de coordenação quando uma falha afeta múltiplos atores. Essa distinção é relevante porque a expansão da conectividade pode aumentar o valor assistencial da informação, mas também ampliar a superfície de exposição se não vier acompanhada de controles proporcionais.

A literatura técnica sobre segurança de APIs reforça essa preocupação. Em arquiteturas baseadas em serviços e integrações, riscos como autorização inadequada em nível de objeto, autenticação frágil, excesso de exposição de dados, ausência de inventário e consumo inseguro de APIs deixam de ser problemas periféricos e passam a integrar a própria sustentabilidade regulatória da Saúde Digital [5]. No caso brasileiro, essa discussão precisa ser situada em um sistema de saúde amplo, federativo e desigual, no qual o mesmo fluxo nacional pode depender de estabelecimentos com maturidades muito diferentes.

O problema investigado neste artigo é: em que medida as evidências públicas disponíveis indicam condições regulatórias, organizacionais e técnicas para sustentar a interoperabilidade segura na Saúde Digital brasileira? O objetivo foi analisar a governança da interoperabilidade segura na Saúde Digital brasileira, com foco em regulação, conformidade legal e cibersegurança.

2 MÉTODOS

Foi realizado estudo documental-comparativo, com análise descritiva de dados secundários. Foram utilizadas três frentes de evidência. A primeira foi composta por tabelas agregadas da Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Estabelecimentos de Saúde Brasileiros (TIC Saúde), nos anos disponíveis entre 2018 e 2024. A segunda utilizou dados abertos da RNDS, competência 202601, consultados em 6 de maio de 2026, agregados por unidade federativa e tipo de registro. A terceira reuniu documentos institucionais nacionais e internacionais sobre interoperabilidade, segurança, conformidade, maturidade digital, alertas e governança setorial [6-14].

Na TIC Saúde, foram priorizadas variáveis diretamente relacionadas à tese do artigo: digitalização básica, interoperabilidade declarada, política de segurança da informação e controles associados à confiança digital, especialmente criptografia de base de dados, certificado digital e autenticação de dois fatores. As medidas temporais foram calculadas por diferença direta entre o percentual final e o percentual inicial disponível, em pontos percentuais. Não foram aplicados testes inferenciais, pois o objetivo não foi estimar causalidade ou significância estatística, mas organizar evidências públicas agregadas em uma leitura regulatória.

Para evitar ambiguidade metodológica, as medidas-resumo apresentadas no artigo foram tratadas como operacionalizações descritivas dos autores a partir de tabelas agregadas oficiais. Não são propostas como indicadores oficiais, instrumentos validados ou métricas do Cetic.br ou do Ministério da Saúde. A digitalização básica (DB) foi tomada como condição mínima de registro eletrônico; a medida de prontidão para interoperabilidade segura (IPIS) agregou, por média simples, três controles associados à proteção e confiança digital; a medida de descompasso entre digitalização e interoperabilidade segura (IDIS) expressou a diferença entre DB e IPIS; e a medida de autenticação forte (IAF) focalizou certificado digital e autenticação de dois fatores. A média simples foi adotada por parcimônia, sem atribuir pesos normativos não observados nas fontes públicas. O Quadro 1 explicita a construção usada neste recorte.

A interpretação dessas medidas é deliberadamente conservadora. O IPIS não mede segurança real de um estabelecimento, não substitui auditoria técnica e não permite inferir maturidade completa de cibersegurança. O IDIS tampouco identifica vulnerabilidade individual; ele apenas indica distância agregada entre a existência de registro eletrônico e a presença de controles mínimos selecionados. O uso das medidas-resumo busca tornar visível uma assimetria relevante para a governança: a digitalização pode avançar mais rapidamente do que a capacidade institucional de

Quadro 1. Operacionalização das medidas-resumo utilizadas no artigo

Medida	Construção operacional	Leitura analítica
DB	Percentual de estabelecimentos com sistema eletrônico para registro das informações dos pacientes (TIC Saúde, B0).	Digitalização básica.
IPIS	Média simples dos percentuais de criptografia da base de dados, certificado digital e autenticação de dois fatores (TIC Saúde, A10).	Prontidão para interoperabilidade segura.
IDIS	Diferença direta entre DB e IPIS, em pontos.	Descompasso entre digitalização e prontidão segura.
IAF	Média simples dos percentuais de certificado digital e autenticação de dois fatores (TIC Saúde, A10).	Força de identificação e acesso.
Variação temporal	Diferença direta entre percentual final e inicial, em pontos percentuais; medidas com duplo fator começam em 2019.	Mudança no período observado.
Estratos de 2024	DB, IPIS, IDIS e IAF calculados para total, setor público, privado, Unidades Básicas de Saúde (UBS), não UBS, capital e interior.	Desigualdade institucional.
Participação RNDS	Registros de cada tipo divididos pela soma dos seis tipos analisados: RIA, RIRA, RAC, REL, RPM e atestados.	Composição funcional da rede.

Fonte: Elaborado pelos autores (2026), a partir das tabelas oficiais da TIC Saúde [6] e dos dados abertos da RNDS [7].

sustentar interoperabilidade segura.

Na RNDS, foram analisados seis tipos de registros públicos agregados: Registros de Imunobiológicos Administrados (RIA), Registros de Informações de Regulação Assistencial (RIRA), Registros de Atendimento Clínico (RAC), Registros de Exames Laboratoriais (REL), Registros de Prescrição de Medicamento (RPM) e atestados. A participação de cada tipo foi calculada pela divisão do seu volume pela soma dos seis tipos observados. Essa métrica não avalia qualidade, completude, utilidade clínica ou segurança do dado; ela descreve a composição funcional pública da rede na competência analisada.

A análise documental foi organizada por categorias compatíveis com a pergunta do estudo: base legal e regulatória, padrões de interoperabilidade, identidade e controle de acesso, auditoria e rastreabilidade, resposta a incidentes, orientação setorial, requisitos para fornecedores e transparência da cadeia de software. A comparação internacional teve função heurística, voltada a identificar instrumentos de governança documentados publicamente, e não a classificar países ou afirmar superioridade institucional. O estudo utilizou apenas dados públicos, secundários e agregados, sem identificação de indivíduos ou estabelecimentos.

3 RESULTADOS

A Tabela 1 apresenta os principais insumos empíricos usados para construir as medidas-resumo de prontidão e descompasso.

A Tabela 1 mostra que a digitalização dos estabelecimentos cresceu mais rapidamente do que a institucionalização da interoperabilidade e da segurança. Entre 2018 e 2024, a digitalização básica passou de 73,2% para 91,6%, enquanto a interoperabilidade declarada passou de 15,3% para 26,1%. A política de segurança também avançou, mas alcançou 41,6% em 2024, permanecendo abaixo da digitalização básica. O mesmo ocorreu com controles selecionados: criptografia de base chegou a 45,6%, certificado digital a 57,4% e autenticação de dois fatores a 21,8%. O conjunto sugere avanço simultâneo, porém assimétrico, entre informatização, interoperabilidade declarada e mecanismos mínimos de confiança digital. Esses insumos sustentam as medidas-resumo apresentadas a seguir.

Tabela 1. Insumos selecionados de digitalização, interoperabilidade e segurança, TIC Saúde 2018-2024

Insumo	Inicial	Final	Variação
Digitalização básica	73,2% (2018)	91,6% (2024)	+18,4 p.p.
Interoperabilidade declarada	15,3% (2018)	26,1% (2024)	+10,8 p.p.
Política de segurança	23,0% (2018)	41,6% (2024)	+18,6 p.p.
Criptografia de base	29,6% (2018)	45,6% (2024)	+16,0 p.p.
Certificado digital	44,7% (2018)	57,4% (2024)	+12,7 p.p.
Autenticação de dois fatores	7,0% (2019)	21,8% (2024)	+14,8 p.p.

Fonte: Elaborado pelos autores (2026), a partir das tabelas oficiais da TIC Saúde 2018-2024 [6].

Tabela 2. Medidas-resumo descritivas por estrato selecionado, TIC Saúde 2024

Estrato	DB	IPIS	IDIS	IAF
Total	91,6	41,6	50,1	39,6
Público	90,2	24,4	65,8	19,3
Privado	92,8	56,2	36,6	56,9
UBS	96,5	23,5	73,0	18,4
Não UBS	89,1	50,9	38,3	50,4
Capital	92,5	56,6	35,9	57,2
Interior	91,4	37,2	54,2	34,4

Fonte: Elaborado pelos autores (2026), a partir das tabelas oficiais da TIC Saúde 2024 [6].

Tabela 3. Composição nacional dos registros analisados da RNDS, competência 202601

Tipo de registro	Registros	Part.
Vacinação/RIA	1,63 bi	49,9%
Regulação assistencial/RIRA	944,0 mi	28,8%
Atendimento clínico/RAC	564,8 mi	17,2%
Exames laboratoriais/REL	76,1 mi	2,3%
Prescrição de medicamento/RPM	50,9 mi	1,6%
Atestados	7,5 mi	0,2%

Fonte: Elaborado pelos autores (2026), a partir dos dados abertos da RNDS [7] (competência 202601, consulta em 6 de maio de 2026).

A Tabela 2 apresenta medidas-resumo descritivas por estrato selecionado em 2024, permitindo observar onde a digitalização básica não se converte em prontidão segura.

A Tabela 2 evidencia que a baixa prontidão não é homogênea. O IPIS total foi 41,6 pontos, mas caiu para 24,4 no setor público, 23,5 nas UBS e 37,2 no interior. Nesses mesmos estratos, o IDIS foi maior, chegando a 65,8 pontos no setor público e 73,0 nas UBS. A leitura mais relevante não é a comparação isolada de um estrato com outro, mas a distância entre digitalização básica e controles de confiança. As UBS, por exemplo, apresentaram DB de 96,5 pontos, mas IPIS de 23,5 e IAF de 18,4; isso indica que a presença de registro eletrônico não deve ser confundida com prontidão para troca segura de dados. O contraste com setor privado, não UBS e capital indica que a interoperabilidade nacional tende a operar sobre uma ponta institucionalmente desigual.

A Tabela 3 apresenta a composição nacional dos tipos de registro analisados na RNDS, na competência 202601.

A Tabela 3 mostra que os seis tipos analisados somaram 3.278.268.583 registros. A vacinação concentrou 49,9% do total, seguida por regulação assistencial (28,8%) e atendimento clínico (17,2%). Exames laboratoriais, prescrição de medicamento e atestados tiveram participações menores. A composição indica que a rede deve ser observada não apenas pelo volume agregado de registros, mas pelos tipos de dado e pelas finalidades assistenciais efetivamente presentes em seus fluxos [7]. Do ponto de vista de governança, esse resultado impede tratar a RNDS como bloco funcional homogêneo: fluxos de imunização, regulação, atendimento clínico, exames, prescrição e atestados exigem perfis distintos de autenticação, autorização, auditoria, retenção e resposta a incidentes.

A análise documental mostrou que a arquitetura brasileira possui base normativa e institucional relevante, especialmente pela RNDS, Guia RNDS/FHIR, Programa SUS Digital, Índice Nacional de Maturidade em Saúde Digital e apoio transversal de estruturas como Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) e Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). Entretanto, no corpus consultado, não foi identificada evidência pública suficiente de uma estrutura setorial de cibersegurança em saúde com função equivalente a CSOC, SOC, CERT ou CSIRT dedicado ao setor. Em contraste, o Reino Unido documenta instrumentos como o Data Security and Protection Toolkit e canais de alertas cibernéticos do NHS, enquanto os Estados Unidos apresentam produtos setoriais do Health Sector Cybersecurity Coordination Center (HC3) e requisitos de segurança associados ao Trusted Exchange Framework and Common Agreement (TEFCA) [8-14].

O recorte técnico-regulatório também indicou três pontos sensíveis para a governança. Primeiro, a interoperabilidade baseada em APIs amplia a superfície de risco ao expor endpoints, objetos, identificadores, funções e integrações entre sistemas. A literatura técnica da Open Web Application Security Project (OWASP) para APIs destaca riscos como falhas

de autorização em nível de objeto, autenticação quebrada, autorização funcional insuficiente, inventário inadequado e consumo inseguro de APIs, pontos diretamente relevantes para fluxos de dados sensíveis em saúde [5,15]. Segundo, padrões historicamente incorporados à Informática em Saúde também podem conter ou carregar vulnerabilidades relevantes. O Digital Imaging and Communications in Medicine (DICOM) é citado aqui como exemplo de padrão setorial amplamente usado, não como foco do artigo: a vulnerabilidade CVE-2019-11687, associada ao DICOM Part 10 File Format, apresenta na National Vulnerability Database (NVD) pontuação Common Vulnerability Scoring System (CVSS) v3.0 de 7,8, classificada como alta, com impactos altos sobre confidencialidade, integridade e disponibilidade [16, 17]. Terceiro, a cadeia de software conectada à Saúde Digital torna recomendável maior transparência sobre componentes, versões e dependências [18,19].

Quadro 2. Síntese interpretativa dos achados e implicações regulatórias

Achado	Implicação para governança
Digitalização básica maior que interoperabilidade e política de segurança.	Definir piso mínimo de interoperabilidade segura para sistemas conectados.
Controles de confiança digital menores no setor público, nas UBS e no interior.	Associar requisitos de segurança a financiamento, capacitação e apoio técnico.
RNDS concentrada em fluxos funcionais específicos, como vacinação e regulação.	Governar por tipo de fluxo, finalidade assistencial e criticidade do dado.
Interoperabilidade por APIs amplia superfície de risco.	Manter inventário de endpoints, autenticação, autorização, testes e gestão de consumo de APIs.
Padrões e componentes podem carregar vulnerabilidades conhecidas.	Vincular padrões, bibliotecas e versões a monitoramento de vulnerabilidades e resposta coordenada.
SBOM é oportunidade de governança, não solução isolada.	Experimentar fluxo proporcional de transparência de componentes para sistemas conectados à RNDS.
Arquitetura nacional existe, mas capacidade setorial documentada é limitada.	Fortalecer mecanismos setoriais de orientação, avaliação de conformidade e resposta a incidentes.

Fonte: Elaborado pelos autores (2026).

A referência ao DICOM tem função analítica limitada e precisa. Não se afirma que o padrão DICOM seja inadequado, nem que a RNDS esteja exposta à vulnerabilidade citada. O ponto é outro: padrões consolidados em Informática em Saúde, inclusive aqueles amplamente incorporados à prática assistencial e a equipamentos, podem depender de implementações, bibliotecas, componentes e versões com vulnerabilidades conhecidas. Para a governança, isso desloca a atenção de uma pergunta binária sobre adotar ou não adotar padrões para uma pergunta operacional: como manter inventário, monitoramento, atualização e resposta quando padrões e componentes atravessam múltiplos fornecedores e serviços.

Nesse contexto, o Software Bill of Materials (SBOM) é apresentado como proposta de instrumento, não como resultado empírico do estudo. Seu papel potencial é iniciar um fluxo de governança para softwares conectados à RNDS, especialmente em cenários de habilitação, manutenção ou resposta coordenada a vulnerabilidades. A utilidade não estaria em exigir listas formais sem capacidade de uso, mas em permitir que componentes, dependências e versões sejam conhecidos, atualizados e relacionados a alertas públicos de vulnerabilidade, de forma proporcional ao porte e ao risco dos sistemas conectados [18,19].

4 DISCUSSÃO

Os achados sustentam a leitura de que a interoperabilidade segura é um problema de governança e conformidade, não apenas de conectividade técnica. A expansão da digitalização básica para 91,6% dos estabelecimentos em 2024 não foi acompanhada por patamar equivalente de interoperabilidade declarada, política de segurança ou controles robustos de confiança digital. Esse descompasso importa para a regulação porque a LGPD exige que o tratamento de dados pessoais sensíveis seja sustentado por responsabilização, segurança e finalidade adequada [1, 6].

A principal contribuição das medidas-resumo está em organizar essa diferença de forma transparente. O IPIS aproxima controles mínimos de proteção e confiança digital; o IDIS explicita a distância entre digitalização básica e prontidão segura; e o IAF focaliza elementos de identificação e autenticação. Essas medidas não pretendem substituir avaliações técnicas, certificações, auditorias ou métricas oficiais de maturidade. Sua função é estritamente descritiva e analítica: demonstrar que uma política nacional de interoperabilidade pode encontrar uma rede já digitalizada, porém com capacidades desiguais para sustentar segurança, rastreabilidade e conformidade.

A desigualdade entre estratos é central para a discussão. Setor público, UBS e interior são partes essenciais da capilaridade do Sistema Único de Saúde, mas apresentaram menor adoção de criptografia de base, certificado digital e autenticação de dois fatores na TIC Saúde 2024. Se a interoperabilidade nacional avança apoiada em uma ponta institucionalmente desigual, a regulação precisa combinar exigências mínimas com suporte proporcional. Caso contrário, requisitos de segurança podem ser formalmente corretos e operacionalmente excludentes [6].

Esse ponto é particularmente importante para a saúde pública. A exigência de controles de segurança não deve ser compreendida como barreira burocrática para

estabelecimentos com menor capacidade, mas como condição para que a expansão da Saúde Digital não aprofunde assimetrias institucionais. Em termos práticos, o desafio regulatório é combinar requisitos mínimos verificáveis com financiamento, capacitação, orientação técnica e instrumentos graduais de conformidade. A segurança, nesse sentido, precisa ser desenhada como política de sustentação da interoperabilidade, e não como ônus isolado atribuído ao ponto mais frágil da rede.

A composição funcional da RNDS reforça esse ponto. Fluxos de vacinação, regulação assistencial, atendimento clínico, exames, prescrições e atestados não têm o mesmo risco, a mesma finalidade nem o mesmo impacto assistencial. Governar a RNDS apenas pelo volume de registros obscurece diferenças relevantes para autenticação, autorização, auditoria, rastreabilidade e resposta a incidentes. Uma governança madura precisa acompanhar a expansão funcional da rede, e não apenas sua existência formal.

A comparação documental sugere que o Brasil já possui arquitetura de Saúde Digital, mas ainda precisa tornar mais visíveis e permanentes as capacidades setoriais de orientação, alerta e apoio a incidentes. CTIR Gov e CERT.br são referências transversais importantes; contudo, a Saúde Digital tem especificidades clínicas, assistenciais, regulatórias e tecnológicas que justificam mecanismos setoriais de coordenação. A experiência internacional mostra que avaliação de conformidade, alertas públicos, requisitos de segurança e centros de coordenação podem funcionar como instrumentos de governança, não apenas como respostas emergenciais.

A ampliação da superfície de risco por APIs deve ser tratada nesse mesmo plano institucional. Em uma rede interoperável, falhas de autenticação, autorização, inventário ou consumo de APIs podem extrapolar a aplicação individual e afetar cadeias assistenciais, fornecedores e fluxos nacionais de dados. A literatura técnica da OWASP é útil porque desloca o foco da segurança apenas perimetral para problemas de desenho, governança e operação de APIs. Para a Saúde Digital, isso implica inventário de interfaces, escopo de acesso, gestão de credenciais, testes, monitoramento, trilhas de auditoria e mecanismos de revogação compatíveis com a sensibilidade dos dados tratados [5].

O exemplo do DICOM reforça que o risco não se limita a APIs novas ou sistemas centrais. Padrões maduros, necessários e disseminados também dependem de implementações concretas. A vulnerabilidade CVE-2019-11687 é relevante neste artigo não por deslocar o foco para imagem médica, mas por ilustrar que padrões setoriais podem envolver superfícies técnicas reconhecidas e pontuadas em bases públicas de vulnerabilidade. Uma política de interoperabilidade segura precisa, portanto, considerar ciclo de vida, versões, bibliotecas, componentes e fornecedores, inclusive quando o padrão em si é legítimo e indispensável [16,17].

Do ponto de vista regulatório, um piso nacional mínimo de interoperabilidade segura deveria incluir autenticação forte, gestão de identidade, autorização por perfil e finalidade, trilhas de auditoria, inventário de sistemas, plano de resposta a incidentes, requisitos proporcionais para fornecedores e mecanismos de transparência sobre componentes de software. Nesse desenho, o SBOM não deve ser tratado como solução isolada nem como exigência desconectada da capacidade dos fornecedores. Sua contribuição mais plausível, neste estágio, é servir como proposta e oportunidade inicial para um fluxo de governança dos softwares conectados à RNDS: inventariar componentes, versões e dependências; apoiar gestão de vulnerabilidades; e criar base mínima para respostas coordenadas quando falhas afetarem bibliotecas, módulos ou padrões usados por múltiplos sistemas [18,19].

A adoção de SBOM, se considerada, deveria ser incremental e orientada por risco. Um caminho plausível seria iniciar por sistemas conectados a fluxos mais críticos, por fornecedores com maior escala de integração ou por componentes compartilhados entre múltiplos serviços. Também seria necessário definir quem recebe, protege, atualiza e utiliza essas informações, pois um inventário de componentes pode conter dados sensíveis sobre a arquitetura dos sistemas. Assim, o SBOM é melhor compreendido como parte de um fluxo de governança de cadeia de software, associado a vulnerabilidade, atualização, homologação e resposta, e não como documento estático de conformidade.

O estudo tem limites. Os dados utilizados são secundários, agregados e documentais; portanto, não permitem auditar integrações específicas, fornecedores ou incidentes operacionais. A comparação internacional também não mede desempenho real de segurança entre países. Ainda assim, a convergência entre TIC Saúde, RNDS e análise documental permite sustentar uma conclusão prudente: a interoperabilidade segura depende de maturidade institucional distribuída e de capacidade regulatória para transformar padrões técnicos em rotinas verificáveis de proteção, conformidade e resposta [6,7,12-14]. A contribuição do estudo está em deslocar a interoperabilidade segura de uma agenda meramente técnica para uma agenda regulatória de governança, articulando evidências de adoção tecnológica, composição funcional da RNDS e lacunas documentais de capacidade setorial.

Pesquisas futuras podem aprofundar essa agenda com refinamento metodológico das medidas-resumo, análise por unidade federativa, estudo de maturidade de fornecedores, entrevistas com gestores e avaliação de fluxos específicos da RNDS. Também seria

pertinente diferenciar, em trabalho posterior, requisitos para prontuários eletrônicos, laboratórios, sistemas de imagem, regulação, prescrição e aplicações móveis, pois cada classe de sistema combina riscos, dependências e responsabilidades distintas. Esses aprofundamentos excedem o escopo deste artigo, mas decorrem diretamente da estratégia de não tratar interoperabilidade, segurança e conformidade como dimensões separadas.

5 CONCLUSÕES

A governança da interoperabilidade segura na Saúde Digital brasileira deve ser compreendida como agenda regulatória, organizacional e técnica. A digitalização avançou, mas controles essenciais à confiança digital permanecem desigualmente distribuídos, especialmente no setor público, nas UBS e no interior. A RNDS, por sua vez, apresenta composição funcional heterogênea, o que exige governança orientada por tipo de dado, finalidade assistencial e capacidade local de sustentação.

Para que a interoperabilidade seja compatível com proteção de dados, segurança cibernética e conformidade legal, o país precisa combinar padrões técnicos com mecanismos permanentes de governança setorial. Isso inclui requisitos mínimos proporcionais, apoio técnico, capacitação, auditoria, resposta a incidentes, gestão de fornecedores e transparência da cadeia de software. O SBOM, nesse cenário, é uma proposta de instrumento possível para iniciar governança de componentes e dependências, não uma solução isolada.

A contribuição do artigo é mostrar que segurança, regulação e interoperabilidade devem ser tratadas como dimensões inseparáveis da Saúde Digital brasileira. A agenda futura deve aprofundar o refinamento metodológico das medidas-resumo, ampliar a análise territorial e setorial e transformar requisitos técnicos em rotinas verificáveis de governança para os diferentes tipos de sistemas conectados à RNDS.

Contribuição dos autores. Os autores contribuíram igualmente em todas as etapas de construção do artigo: concepção e delineamento do estudo; coleta, análise e interpretação dos dados; redação e revisão crítica do manuscrito; e aprovação da versão final.

Financiamento. Os autores não declararam fonte de financiamento.

Disponibilidade de dados e materiais. Os autores não declararam a disponibilidade dos dados e materiais da pesquisa.

Conflitos de interesse. Os autores não declararam conflitos de interesse.

Declaração de uso de IA. Foi utilizada ferramenta de IA generativa como apoio editorial para adaptação de trabalho acadêmico prévio ao formato do CBIS, organização do manuscrito, condensação textual e revisão de clareza. A ferramenta não foi atribuída como autora, não gerou dados, resultados ou referências novas e não substitui a responsabilidade dos autores.

REFERÊNCIAS

1. Brasil. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais [Internet]. Brasília: Presidência da República; 2018 [citado 2026 out 18]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
2. Brasil. Ministério da Saúde. Portaria nº 1.434, de 28 de maio de 2020. Institui o Programa Conecte SUS e a Rede Nacional de Dados em Saúde [Internet]. Brasília: Ministério da Saúde; 2020 [citado 2026 nov 24]. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2020/prt1434_01_06_2020_rep.html
3. Brasil. Ministério da Saúde. Guia de Implementação da RNDS: FHIR v4.0.1 [Internet]. Brasília: Ministério da Saúde; 2022 [citado 2026 abr 29]. Disponível em: https://rnds-fhir.saude.gov.br/ImplementationGuide-rnds.html
4. Health Level Seven International. Security and privacy module. In: HL7 FHIR Release 4. Ann Arbor: HL7 International; 2019 [citado 2026 abr 29]. Disponível em: https://hl7.org/fhir/R4/security.html.
5. Open Web Application Security Project. OWASP API Security Top 10: 2023. OWASP Foundation; 2023 [citado 2026 abr 29]. Disponível em: https://owasp.org/www-project-api-security/.
6. Núcleo de Informação e Coordenação do Ponto BR. Pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros (TIC Saúde), 2018-2024: tabelas [Internet]. São Paulo: NIC.br; 2024 [citado 2026 nov 24]. Disponível em: https://cetic.br/pt/pesquisa/saude/
7. Brasil. Ministério da Saúde. Secretaria de Informação e Saúde Digital. Rede Nacional de Dados em Saúde (RNDS): dados abertos [Internet]. Brasília: Ministério da Saúde; 2026 [citado 2026 maio 6]. Disponível em: https://dadosabertos.saude.gov.br/dataset/mgdi-rede-nacional-de-dados-em-saude-rnds
8. Brasil. Ministério da Saúde. Portaria GM/MS nº 3.232, de 1º de março de 2024. Institui o Programa SUS Digital [Internet]. Brasília: Ministério da Saúde; 2024 [citado 2026 nov 24]. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2024/prt3232_04_03_2024.html
9. Brasil. Ministério da Saúde. Secretaria de Informação e Saúde Digital. Manual instrutivo do Programa SUS Digital [Internet]. Brasília: Ministério da Saúde; 2024 [citado 2026 out 18]. Disponível em: https://www.gov.br/saude/pt-br/centrais-de-conteudo/publicacoes/guias-e-manuais/2024/manual-instrutivo-do-programa-sus-digital

10. Brasil. Gabinete de Segurança Institucional. CTIR Gov: Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo [Internet]. Brasília: GSI; 2025 [citado 2026 abr 29]. Disponível em: https://www.gov.br/ctir/pt-br

11. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. CERT.br [Internet]. São Paulo: NIC.br; 2025 [citado 2026 abr 29]. Disponível em: https://cert.br/

12. NHS England. Data Security and Protection Toolkit. Leeds: NHS England; 2024 [citado 2026 abr 29]. Disponível em: https://www.dsptoolkit.nhs.uk/.

13. NHS England. NHS Cyber Alerts. Leeds: NHS England; 2024 [citado 2026 abr 29]. Disponível em: https://digital.nhs.uk/cyber-alerts.

14. U.S. Department of Health and Human Services. Health Sector Cybersecurity Coordination Center (HC3). Washington, DC: HHS; 2025 [citado 2026 abr 29]. Disponível em: https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html.

15. Knight A. Playing with FHIR: hacking and securing FHIR APIs. Approov; 2021 [citado 2026 abr 30]. Disponível em: https://confluence.hl7.org/download/attachments/94650307/2021-10-21%20Playing%20with%20FHIR%20Report%20by%20Alissa%20Knight%20sponsored%20by%20Approov.pdf.

16. CISA. ICS-ALERT-19-162-01: DICOM Standard in Medical Devices. Washington, DC: Cybersecurity and Infrastructure Security Agency; 2019 [citado 2026 abr 29]. Disponível em: https://www.cisa.gov/news-events/ics-alerts/ics-alert-19-162-01.

17. National Institute of Standards and Technology. CVE-2019-11687 detail. National Vulnerability Database [Internet]. Gaithersburg (MD): NIST; 2019 [citado 2026 maio 17]. Disponível em: https://nvd.nist.gov/vuln/detail/CVE-2019-11687

18. Open Web Application Security Project. OWASP CycloneDX (ECMA-424): CycloneDX Bill of Materials Specification. OWASP Foundation; 2025 [citado 2026 abr 29]. Disponível em: https://owasp.org/www-project-cyclonedx/.

19. Cybersecurity and Infrastructure Security Agency et al. A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity. Washington, DC: CISA; 2025 [citado 2026 abr 29].

NOTAS EDITORIAIS

O Journal of Health Informatics é uma publicação científica mantida pela Sociedade Brasileira de Informática em Saúde, associação científica sem fins lucrativos dedicada ao desenvolvimento da Informática em Saúde e da Saúde Digital no Brasil. O processo editorial é conduzido com independência científica, sem interferência institucional, comercial ou de patrocinadores, e segue as boas práticas internacionais de ética em publicação científica.

Este artigo foi avaliado por pares, em sistema duplo-cego, por especialistas da área. A equipe editorial usou ferramentas de inteligência artificial, com supervisão humana, na triagem inicial, na conferência do texto, das referências e dos números e, quando necessário, no redesenho de figuras, quadros e tabelas, aprovado pelos autores na prova. As ferramentas e as salvaguardas estão na Política de uso de inteligência artificial da revista. As decisões editoriais foram tomadas por pessoas.

SBIS Sociedade Brasileira de Informática em Saúde