Consentimento Digital Verificável e Auditabilidade em Sistemas de Informação em Saúde: um Modelo Híbrido com DID/VC, ICP-Brasil e Evidências Imutáveis

Otávio Alves Gomes[1], **Carlos Frederico Marcelo da Cunha Cavalcanti**[1]

[1] Departamento de Ciência da Computação (DECOM)
Universidade Federal de Ouro Preto (UFOP) – Ouro Preto, MG – Brazil

otavio.gomes@aluno.ufop.edu.br, cfmcc@ufop.edu.br

Resumo. *Sistemas de informação em saúde exigem mutabilidade dos dados clínicos e governança de acesso e consentimento. Contudo, armazenar conteúdo clínico em trilhas imutáveis conflita com requisitos de ciclo de vida, enquanto abordagens puramente off-chain tendem a gerar evidências pouco verificáveis. Propomos o gFHIR-HA, uma arquitetura híbrida que mantém recursos FHIR off-chain e registra on-chain evidências append-only. A arquitetura combina SSI (DID/VC) e PKI (incluindo ICP-Brasil) e mapeia requisitos da LGPD para decisões arquiteturais. Avaliamos uma PoC em Hyperledger Fabric com eventos sintéticos, reportando métricas de latência e tamanho de evidências.*

Abstract. *Healthcare information systems require clinical data mutability and strong governance of access and consent. However, storing clinical content on immutable ledgers conflicts with data-lifecycle requirements, while purely off-chain approaches often yield weak, non-verifiable evidence. We propose gFHIR-HA, a hybrid architecture that keeps FHIR resources off-chain and records append-only on-chain governance evidence. The architecture combines SSI (DID/Verifiable Credentials) and PKI, and maps LGPD requirements to architectural decisions. We evaluate a proof-of-concept on Hyperledger Fabric with synthetic events, reporting latency and evidence-size metrics.*

1. Introdução

A disponibilidade de dados clínicos íntegros e atualizados é crítica para diagnóstico, continuidade do cuidado e uso secundário responsável [Gordon and Catalini 2018]. Com a digitalização e o compartilhamento interinstitucional, o titular frequentemente tem visibilidade limitada sobre acessos e finalidades de uso, o que afeta confiança e responsabilização [Gordon and Catalini 2018, Nissenbaum 2010]; além disso, mesmo com desidentificação, o risco de reidentificação depende do contexto [El Emam et al. 2011], reforçando a necessidade de consentimento verificável, revogação e auditabilidade.

No Brasil, a LGPD estabelece obrigações para o tratamento de dados pessoais sensíveis, incluindo dados de saúde, e a ICP-Brasil oferece uma PKI regulamentada para assinaturas digitais e autenticidade documental. Em cenários multi-institucionais, DID e *Verifiable Credentials* (VC), no contexto de SSI, permitem representar atributos/papéis e suportar verificações criptográficas interoperáveis.

Abordagens baseadas em *blockchain*/DLT têm sido exploradas para rastreabilidade, sobretudo no registro de eventos de acesso [Azaria et al. 2016, Gordon and Catalini 2018, Zhang et al. 2018]. Contudo, impor imutabilidade ao conteúdo clínico conflita com requisitos de ciclo de vida (retificação, eliminação e revogação). Assim, o desafio é separar conteúdo clínico (mutável) de evidências de governança (imutáveis), de forma compatível com regulações e com sistemas legados.

Partindo da premissa de que a imutabilidade deve recair sobre evidências (eventos, provas, *hashes* e auditoria), propomos o gFHIR-HA: uma arquitetura híbrida em que recursos FHIR permanecem *off-chain* sob governança institucional, enquanto uma trilha *append-only on-chain* registra emissão/revogação de consentimento e decisões de acesso. As contribuições incluem a arquitetura e o protocolo de ciclo de vida do consentimento, o mapeamento LGPD–arquitetura e uma prova de conceito com métricas de latência e tamanho de evidências. O artigo organiza-se em fundamentos, trabalhos relacionados, descrição do modelo, mapeamento regulatório, prova de conceito e conclusão.

2. Fundamentação Teórica e Tecnológica

2.1. DID e Verifiable Credentials (SSI)

Identificadores Descentralizados (DIDs) e *Verifiable Credentials* (VCs) são padrões do W3C frequentemente associados ao paradigma de Identidade Auto-Soberana (*Self-Sovereign Identity* – SSI) [W3C 2022, W3C 2025, Bai et al. 2022]. DIDs fornecem identificadores persistentes resolvíveis para material criptográfico e metadados de interação, enquanto VCs permitem representar atributos, papéis e autorizações de forma criptograficamente verificável e interoperável, com suporte a verificação por terceiros e revogação. No gFHIR-HA, DID/VC são utilizados para identificar atores (titular, profissional e instituição), expressar papéis/permissões e suportar consentimento verificável e revogável.

2.2. PKI, ICP-Brasil e assinaturas digitais

Infraestruturas de Chaves Públicas (PKI) baseadas em certificados X.509 sustentam autenticação forte e assinatura digital, reforçando integridade e não repúdio. No Brasil, a PKI regulamentada é a ICP-Brasil (MP nº 2.200-2/2001), com normativos e práticas consolidadas para validade jurídico-probatória [Brasil 2001, ITI 2008]. Neste trabalho, PKI/ICP-Brasil é empregada para atos selecionados que demandam maior garantia jurídica, complementando SSI: PKI/ICP para assinatura e não repúdio; DID/VC para credenciais interoperáveis e autorização/consentimento em fluxos dinâmicos.

2.3. LGPD e dados de saúde

A LGPD classifica dados de saúde como dados pessoais sensíveis e estabelece princípios e obrigações para seu tratamento [Brasil 2018]. Para este trabalho, destacam-se: princípios (Art. 6º), consentimento e revogação (Art. 8º), dados sensíveis (Art. 11), direitos do titular (Art. 18) e segurança (Art. 46), motivando mecanismos de controle verificável de consentimento, rastreabilidade de acessos e revogação operacional, em diálogo com a literatura sobre privacidade contextual e reidentificação em dados de saúde [Nissenbaum 2010, El Emam et al. 2011].

2.4. FHIR e o recurso Consent

HL7 FHIR é um padrão amplamente adotado para interoperabilidade em saúde, baseado em recursos trocados via APIs REST em JSON/XML [HL7 International 2019]. O recurso `Consent` representa decisões de consentimento e restrições de uso/compartilhamento [HL7 International 2026], com evidências de viabilidade em cenários reais e em arquiteturas de compartilhamento seguro de dados clínicos [Voronov et al. 2024, Zhang et al. 2018]. Entretanto, FHIR/`Consent` não define, por si só, identidade interoperável, verificabilidade criptográfica e trilha auditável de decisões de acesso. O gFHIR-HA preserva a interoperabilidade FHIR e adiciona DID/VC, PKI selecionada e evidências *append-only* para auditabilidade e governança.

3. Trabalhos Relacionados

Esta seção revisa trabalhos relevantes em três frentes principais: uso de blockchain/DLT em saúde, integração com o padrão FHIR e abordagens baseadas em identidade descentralizada para governança de consentimento.

Tabela 1. Comparação entre abordagens existentes e o modelo proposto

Abordagem	FHIR	SSI	PKI	Consent	Auditoria
MedRec [Azaria et al. 2016]	–	–	–	Parcial	Sim
FHIRChain [Zhang et al. 2018]	Sim	Parcial	–	Parcial	Sim
SSI em saúde [Bai et al. 2022]	–	Sim	–	Parcial	Limitado
Plataformas de consentimento [Brückner et al. 2025]	Parcial	Parcial	–	Sim	Parcial
gFHIR-HA (proposto)	Sim	Sim	Sim	Sim	Sim

A literatura sobre *blockchain*/DLT em saúde aponta benefícios potenciais relacionados à auditabilidade, integridade e compartilhamento controlado de dados, mas também destaca desafios e *trade-offs* envolvendo privacidade, escalabilidade e governança [Agbo et al. 2019, Azaria et al. 2016, Gordon and Catalini 2018, Zhang et al. 2018]. Em muitos desses trabalhos, a DLT é utilizada como um *ledger* imutável para registro de eventos, por exemplo, acessos e autorizações, enquanto o conteúdo clínico permanece armazenado em repositórios externos, dada a sensibilidade desses dados e a necessidade de um ciclo de vida governável.

MedRec [Azaria et al. 2016] é frequentemente citado como um trabalho seminal no gerenciamento de acesso a dados médicos utilizando blockchain. Gordon e Catalini [Gordon and Catalini 2018] discutem a transição para modelos de interoperabilidade orientados ao paciente e identificam a imutabilidade como um dos mecanismos possíveis para suportar confiança entre instituições, ao mesmo tempo em que destacam barreiras de adoção e riscos associados à privacidade.

FHIRChain [Zhang et al. 2018] aproxima tecnologias blockchain da interoperabilidade clínica por meio do padrão FHIR, demonstrando um caso de compartilhamento de dados clínicos com identidade digital. Embora relevante, a proposta concentra-se em um cenário específico e não discute em profundidade (i) requisitos de revogação e auditoria

ao longo do ciclo de vida do consentimento, nem (ii) mecanismos de integração com infraestruturas jurídicas e operacionais, como PKIs regulamentadas (p.ex., ICP-Brasil), em consonância com legislações de proteção de dados.

Em paralelo, trabalhos sobre SSI (*Self-Sovereign Identity*) em saúde exploram DID/VC e modelos descentralizados de identidade, incluindo cenários envolvendo IoMT [Bai et al. 2022]. Entretanto, muitos desses trabalhos enfatizam aspectos de identidade e autenticação, sem tratar de forma sistemática o ciclo de vida completo do consentimento — incluindo emissão, verificação, uso, revogação e auditoria — nem os requisitos mínimos de rastreabilidade e responsabilização em ambientes interinstitucionais.

Por fim, iniciativas recentes de plataformas de consentimento em saúde reforçam a centralidade de consentimento granular, revogável e auditável, bem como o uso de FHIR e técnicas de pseudonimização [Brückner et al. 2025]. Em síntese, a literatura existente aborda parcialmente aspectos de interoperabilidade, identidade digital e registro imutável de eventos, mas raramente integra esses elementos em uma arquitetura coerente que contemple simultaneamente governança de consentimento, verificabilidade criptográfica e alinhamento com infraestruturas regulatórias de confiança digital.

Em contraste com essas abordagens, este trabalho propõe uma arquitetura híbrida de referência que integra: (i) PKI regulamentada, com ênfase no caso brasileiro da ICP-Brasil; (ii) mecanismos de identidade descentralizada baseados em DID/VC (SSI); (iii) evidências imutáveis registradas em um *ledger append-only*; e (iv) separação estrita entre conteúdo clínico FHIR (*off-chain*) e trilha de evidências (*on-chain*), suportada por uma camada transversal de controle centrada no titular. Essa arquitetura busca estender o modelo de consentimento baseado em FHIR ao incorporar propriedades de verificabilidade, rastreabilidade e governança do consentimento adequadas a ambientes interinstitucionais de compartilhamento de dados em saúde.

4. Modelo gFHIR (gFHIR-HA)

Este trabalho propõe o gFHIR-HA (*governed FHIR hybrid architecture*), uma arquitetura de referência híbrida para governança verificável de consentimento no compartilhamento de dados de saúde. O modelo preserva a interoperabilidade clínica baseada em FHIR e introduz uma camada de controle centrada no titular, capaz de emitir, verificar e revogar consentimentos de forma rastreável, sem impor imutabilidade ao conteúdo clínico sensível.

O núcleo do gFHIR-HA é a separação explícita entre (i) conteúdo clínico *off-chain*, armazenado em repositórios compatíveis com FHIR e sujeito ao ciclo de vida regulatório (retificação, retenção e eliminação), e (ii) evidências de governança *on-chain*, registradas em trilha *append-only* por meio de eventos e provas criptográficas (p.ex., *hashes* de versões, decisões de acesso e revogações). Essa separação viabiliza auditabilidade e responsabilização sem expor dados de saúde na camada imutável.

De forma conceitual, o modelo integra quatro componentes complementares:

$$\text{gFHIR-HA} = \langle \text{FHIR},\ \text{SSI}\,(\text{DID/VC}),\ \text{PKI},\ \text{Ledger}_{\text{evid}} \rangle$$

onde FHIR define a interoperabilidade semântica dos recursos clínicos; SSI (DID/VC) provê identidade interoperável e credenciais verificáveis para representar pa-

Figura 1. Arquitetura conceitual do modelo gFHIR-HA.

péis e autorizações; PKI (incluindo ICP-Brasil como instanciação regulamentada) é utilizada em atos selecionados com maior exigência jurídico-probatória e não repúdio; e Ledger de evidências mantém o registro imutável (append-only) de evidências do ciclo de vida do consentimento.

Na arquitetura, DID/VC suportam autenticação por atributos e verificação de vínculo/papel (p.ex., profissional habilitado e instituição), enquanto a PKI complementa o modelo em cenários que requerem assinatura qualificada e validade jurídico-probatória. O *ledger* registra eventos relevantes de governança (emissão/revogação de consentimento, apresentação/verificação de credenciais, solicitações e decisões de acesso), mantendo apenas metadados mínimos e provas criptográficas, sem armazenar PHI/PII. Assim, o gFHIR-HA compatibiliza interoperabilidade baseada em FHIR com auditabilidade verificável e governança de consentimento centrada no titular, mantendo aderência a requisitos regulatórios e viabilidade incremental em ambientes reais.

4.1. Visão geral da arquitetura

A Figura 1 apresenta a arquitetura conceitual do modelo gFHIR-HA. De forma simplificada, a arquitetura pode ser lida de cima para baixo: aplicações de saúde interagem com repositórios clínicos baseados em FHIR, enquanto mecanismos de identidade descentralizada gerenciam credenciais e autenticação; eventos associados ao ciclo de vida do consentimento são então registrados como evidências criptográficas em um *ledger append-only*, suportado por uma infraestrutura de confiança baseada em PKI. O modelo organiza-se em camadas que separam a representação semântica dos dados clínicos da gestão de identidade e da trilha de evidências associada ao consentimento.

Na camada superior encontram-se as aplicações de saúde, como sistemas hospitalares, prontuários eletrônicos e plataformas de telemedicina. Essas aplicações interagem com repositórios clínicos baseados em FHIR, responsáveis pela representação semântica e interoperabilidade dos dados de saúde.

A camada de identidade utiliza mecanismos baseados em DID e *Verifiable Credentials* para representar titulares, profissionais de saúde e instituições, permitindo apresentação de credenciais verificáveis e autenticação interoperável.

Eventos relacionados ao ciclo de vida do consentimento — como emissão, verificação, uso e revogação — são registrados em um *ledger append-only*, que armazena metadados e provas criptográficas sem expor conteúdo clínico sensível.

A infraestrutura PKI atua como camada de confiança institucional, permitindo assinatura digital qualificada e não repúdio em atos formais associados ao consentimento.

Do ponto de vista funcional, essa arquitetura pode ser compreendida em quatro planos complementares:

1. **Plano de dados clínicos (off-chain)**: repositórios clínicos, documentos e metadados modelados em FHIR;
2. **Plano de identidade e credenciais**: DIDs, VCs e mecanismos de verificação e revogação de credenciais;
3. **Plano de confiança jurídico-documental**: assinaturas digitais baseadas em ICP-Brasil aplicadas a documentos selecionados;
4. **Plano de evidências auditáveis**: trilha imutável *append-only* contendo *hashes* e eventos relacionados ao consentimento.

Além desses componentes tecnológicos, o modelo introduz explicitamente uma camada de governança do consentimento, responsável por definir políticas de autorização, escopo de acesso e condições de revogação no compartilhamento de dados de saúde. Essa camada coordena a interação entre FHIR, identidade descentralizada e registro de evidências criptográficas, garantindo que decisões de acesso sejam verificáveis, auditáveis e alinhadas aos requisitos regulatórios.

4.2. Atores e princípios do modelo

O modelo considera um conjunto de atores típicos do ecossistema de saúde digital. O titular (paciente) é responsável por conceder, revisar e eventualmente revogar consentimentos relacionados ao compartilhamento de seus dados. Profissionais de saúde solicitam acesso aos dados conforme escopo e finalidade definidos, enquanto a instituição de saúde atua como custodiante dos repositórios clínicos e executora das políticas de acesso.

No plano de identidade digital, um emissor de credenciais é responsável por emitir Verifiable Credentials associadas a atributos e papéis, enquanto verificadores validam essas credenciais e evidências de consentimento durante solicitações de acesso. Atores de auditoria e compliance podem inspecionar a trilha de evidências para verificar consistência de eventos e conformidade regulatória.

O modelo adota princípios de projeto voltados à proteção de dados e auditabilidade. Entre eles destacam-se a minimização de dados, evitando armazenamento de PII/PHI na trilha imutável; a separação de responsabilidades, mantendo identidade, dados clínicos e evidências em planos distintos; a auditabilidade por evidência, registrando provas de eventos em vez de conteúdo clínico; a revogabilidade operacional do consentimento; e a interoperabilidade com o padrão FHIR, permitindo integração com sistemas de saúde existentes.

4.3. Separação arquitetural e armazenamento

No modelo gFHIR-HA, dados clínicos sensíveis permanecem em repositórios institucionais *off-chain*, enquanto apenas evidências criptográficas são registradas na trilha imutá-

vel. Essa separação permite conciliar requisitos de privacidade e interoperabilidade com propriedades de auditabilidade.

Nos repositórios clínicos institucionais são armazenados dados pessoais e dados sensíveis de saúde, incluindo prontuários, laudos, imagens e documentos clínicos, bem como vínculos internos entre pacientes e identificadores institucionais. Esses sistemas também implementam políticas locais de retenção, anonimização e eliminação de dados.

A camada de evidências imutáveis registra apenas metadados necessários para auditoria, como identificadores pseudonimizados do titular, *hashes* de documentos ou versões, eventos de emissão ou revogação de consentimento, registros de verificação e acesso autorizado ou negado, além de *timestamps* e identificadores de transação associados às operações realizadas.

4.4. Ciclo de vida do consentimento

No gFHIR-HA, o consentimento é tratado como artefato dinâmico com emissão, verificação/uso e revogação. O titular expressa o consentimento de forma estruturada (compatível com `FHIR Consent`) e a camada de controle registra a autorização e a evidência criptográfica correspondente na trilha *append-only*. Em solicitações de acesso, o solicitante apresenta credenciais verificáveis (papel/finalidade); o sistema valida credenciais, avalia políticas e, se autorizado, libera no repositório *off-chain* apenas o mínimo necessário, registrando a decisão e o evento de auditoria. A revogação ou atualização gera novos eventos, preservando histórico e permitindo auditoria posterior sem armazenar dados clínicos na camada imutável.

5. Compatibilidade com a LGPD

Esta seção formaliza o mapeamento entre requisitos legais e decisões de arquitetura. O objetivo não é substituir análise jurídica, mas demonstrar *compatibilidade funcional* e *accountability by design*.

Tabela 2. Mapeamento LGPD $\times$ mecanismos técnicos da arquitetura proposta

LGPD	Exigência / princípio	Mecanismo na arquitetura	Observação
Art. 6º	Necessidade / minimização	Dados clínicos e PII/PHI *off-chain*; trilha imutável registra apenas metadados, *hashes* e eventos pseudonimizados	Evita exposição indevida na camada imutável
Art. 6º	Segurança / prevenção	Assinaturas digitais, verificações criptográficas, trilha de auditoria *append-only*, controle de acesso contextual	Reforça integridade e detecção de abuso
Art. 6º e Art. 37	Responsabilização / prestação de contas	Registro auditável de operações e decisões de acesso	Facilita auditoria e compliance
Art. 8º	Consentimento e revogação	Consentimento estruturado, registro de evento de emissão/revogação, avaliação de estado vigente no momento do acesso	Revogação impacta acessos futuros
Art. 11	Dados sensíveis (saúde)	Separação entre conteúdo sensível e camada de evidências; políticas de acesso por finalidade/papel	Foco em governança de tratamento
Art. 18	Direitos do titular (p.ex., correção)	Correções/eliminações/bloqueios ocorrem no repositório *off-chain*; trilha registra evidência da ação de governança	Imutabilidade recai sobre evidência, não sobre PHI
Art. 46	Medidas de segurança	Criptografia, gestão de credenciais, logs verificáveis e trilhas de auditoria	Requer implementação institucional adequada

Esse mapeamento não pretende esgotar a interpretação jurídica da LGPD, mas

evidenciar que as decisões arquiteturais do modelo gFHIR-HA foram concebidas para suportar princípios de proteção de dados *by design*.

5.1. Discussão: imutabilidade versus ciclo de vida dos dados

A proposta endereça a tensão entre requisitos regulatórios de proteção de dados e o uso de infraestruturas de registro imutável, discutida em trabalhos sobre privacidade, reidentificação e blockchain em saúde [Gordon and Catalini 2018, Nissenbaum 2010, El Emam et al. 2011].

No modelo proposto, a imutabilidade é aplicada exclusivamente às evidências de governança do tratamento de dados, enquanto a mutabilidade controlada permanece no repositório clínico institucional. Dessa forma, eventos relevantes do ciclo de vida do consentimento, como emissão, verificação, uso e revogação, podem ser registrados como evidências criptográficas verificáveis, sem que dados clínicos sensíveis sejam armazenados na infraestrutura imutável.

Essa abordagem permite preservar simultaneamente duas propriedades frequentemente consideradas difíceis de conciliar. Por um lado, a arquitetura mantém auditabilidade histórica, permitindo verificar o que ocorreu, quando e sob quais condições de autorização. Por outro, preserva governabilidade operacional, possibilitando correção, bloqueio, eliminação, anonimização ou atualização de consentimentos conforme exigido pelo ciclo de vida regulatório dos dados de saúde.

Assim, a imutabilidade não é aplicada ao conteúdo clínico em si, mas às evidências verificáveis das decisões e eventos associados ao seu tratamento, permitindo compatibilizar mecanismos de registro imutável com requisitos de governança e proteção de dados.

6. Análise de segurança

A arquitetura gFHIR-HA envolve mecanismos de interoperabilidade clínica, identidade digital, controle de consentimento e registro auditável de eventos. Por isso, é necessário considerar vetores de ameaça associados ao compartilhamento interinstitucional de dados de saúde, à validação contextual de acesso e à integridade das evidências registradas [Rose et al. 2020]. Esta seção apresenta o modelo de ameaças considerado e discute como as decisões arquiteturais propostas contribuem para reduzir riscos relacionados à autenticidade, integridade, confidencialidade e governança do consentimento.

6.1. Modelo de ameaças

No contexto de compartilhamento de dados clínicos entre instituições, consideram-se ameaças associadas à validade do consentimento, ao controle de acesso, à integridade da trilha de auditoria e à proteção de dados sensíveis. Em particular, destacam-se:

- **Fraude de consentimento**: criação ou alteração indevida de registros para autorizar acessos não legítimos;
- **Repúdio**: contestação posterior da existência ou validade de um consentimento previamente registrado;
- **Acesso fora de escopo**: tentativa de acesso por profissionais ou instituições sem credenciais adequadas ou fora da finalidade autorizada;

- **Adulteração de registros de auditoria**: tentativa de modificar ou remover evidências de eventos relacionados ao compartilhamento de dados;
- **Exposição de dados sensíveis**: vazamento de informações clínicas por armazenamento inadequado em infraestruturas imutáveis;
- **Validação inconsistente de credenciais**: falhas na verificação de papéis, vínculos institucionais ou finalidade declarada entre diferentes organizações.

6.2. Mitigações providas pela arquitetura

O modelo gFHIR-HA incorpora mecanismos destinados a mitigar essas ameaças por meio da combinação entre identidade verificável, assinaturas digitais, registro append-only e separação entre dados clínicos e evidências de governança. A integridade de consentimentos e documentos associados pode ser reforçada por assinaturas digitais e funções de *hash* criptográficas, permitindo verificar se um artefato foi alterado após sua emissão.

A utilização de um *ledger append-only* para registrar eventos de emissão, verificação e revogação de consentimento dificulta a adulteração posterior de registros e fornece uma trilha de evidências verificável para auditoria. Além disso, a verificação de credenciais baseada em *Verifiable Credentials* permite validar atributos como papel profissional, vínculo institucional e finalidade declarada antes da concessão de acesso a dados clínicos, reduzindo o risco de acesso indevido.

Por fim, a arquitetura separa explicitamente o armazenamento de dados clínicos do registro de evidências auditáveis. Informações sensíveis permanecem em repositórios institucionais *off-chain*, enquanto a trilha imutável registra apenas metadados e evidências criptográficas de eventos relevantes. Essa separação reduz riscos de exposição de dados sensíveis e facilita a aplicação de políticas de governança compatíveis com requisitos regulatórios.

7. Resultados da Prova de Conceito

7.1. Cenário de uso

Considera-se o fluxo de exames laboratoriais com compartilhamento para médico assistente/segunda opinião. Após a realização do exame, o laudo é disponibilizado em repositório institucional do laboratório (*off-chain*) e pode ser assinado digitalmente (ICP-Brasil) para reforçar autenticidade e não repúdio. O titular concede consentimento verificável e revogável para que um profissional específico (ou um conjunto de profissionais com credenciais compatíveis) acesse o laudo por finalidade e janela temporal definidas. Cada solicitação de acesso é avaliada por política contextual (papel, finalidade, prazo) e registrada como evidência auditável *append-only*. A revogação gera novo evento e impede acessos subsequentes, preservando rastreabilidade e *accountability* sem impor imutabilidade ao conteúdo clínico.

7.2. Implementação e estratégia de avaliação

A PoC demonstra a viabilidade do fluxo sem depender de integração clínica real. Implementou-se: (i) geração de consentimento estruturado; (ii) cálculo de *hash* de consentimento/documento; (iii) verificação de credenciais (VC) e avaliação de política (escopo/finalidade/prazo); (iv) registro de eventos em trilha *append-only* (com *ledger* baseado em Hyperledger Fabric); e (v) revogação seguida de nova tentativa de acesso.

A avaliação adota simulação com dados sintéticos para contornar barreiras éticas, legais e operacionais associadas a prontuários e logs reais, permitindo controle de variáveis e reprodutibilidade. Essa escolha é consistente com práticas recentes na literatura em SBCAS, nas quais simuladores são utilizados como etapa inicial antes de validações em campo. O código-fonte da PoC está disponível publicamente no GitHub[1].

Como parte da implementação, a Tabela 3 resume os tipos de eventos registrados na trilha de evidências da PoC.

Tabela 3. Tipos de eventos na trilha de evidências do gFHIR (*append-only*).

Evento	Campos principais (evidência)	Observação
`DocAnchored`	*docRef*, *docHash*, *docVersion*, *issuerDID*, *ts*	Âncora de integridade
`DocSigned`	*docRef*, *sigRef*, *issuerICP*, *ts*	Ref. a assinatura
`ConsentIssued`	*consentId*, *subjectPid*, *granteeDID*, *scope*, *purpose*, *validFrom*, *validTo*, *policyVer*, *consentHash*, *ts*	Consentimento verificável
`ConsentRevoked`	*consentId*, *subjectPid*, *revocationReason*, *ts*	Revogação por evento
`CredentialPresented`	*requestId*, *presenterDID*, *credType*, *credStatus*, *ts*	VC papel/vínculo
`AccessRequested`	*requestId*, *subjectPid*, *requesterDID*, *docRef*, *purpose*, *ts*	Pedido de acesso
`AccessDecided`	*requestId*, *decision*, *reasonCode*, *policyVer*, *ts*	Permitido/negado
`EvidenceChained`	*eventId*, *prevHash*, *eventHash*, *ts*	Encadeamento

7.3. Resultados e métricas

As questões de avaliação consideradas foram: (Q1) o modelo preserva auditabilidade sem expor dados sensíveis na trilha imutável? (Q2) o fluxo de consentimento e revogação é verificável e operacionalmente executável? (Q3) qual o *overhead* de verificação e registro de evidências? As Tabelas 4 e 5 sintetizam, respectivamente, os parâmetros do simulador e as métricas obtidas na PoC.

Tabela 4. Parâmetros do simulador de eventos do gFHIR.

Parâmetro	Valores	Descrição
D (dias simulados)	30	Janela temporal do experimento
N_s (titulares)	50	Número de pacientes/titulares
N_p (médicos)	15	Profissionais com VC de papel
N_l (laboratórios)	3	Instituições emissoras de laudos
λ_e (exames por titular)	0.9	Poisson por 30 dias
λ_a (acessos por laudo)	2	Tentativas médias por laudo
P_{share}	0.8	Prob. de compartilhar com médico
P_{revoke}	0.25	Prob. de revogar antes do prazo
P_{unauth}	0.1	Tentativas fora de escopo
T_{valid}	10 dias	Validade típica do consentimento
Propósito (*purpose*)	cuidado / 2ª opinião	Distribuição de finalidades

Tabela 5. Resultados da PoC gFHIR-HA.

Operação	Média	Desvio	N
Cálculo de *hash* (documento/consent.)	< 1 ms	0,1 ms	50
Verificação de VC (papel/vínculo)	143,16 ms	34,78 ms	38
Avaliação de política (escopo/finalidade/prazo)	151,42 ms	30,44 ms	38
Registro de evidência (*append-only*)	158,64 ms	94,53 ms[†]	229
Emissão de consent. (*end-to-end*)	167,10 ms	44,22 ms	–
Revogação (*end-to-end*)	166,37 ms	24,03 ms	–

[†] Desvio elevado por *warm-up* na primeira invocação (máx. 2.867 ms; demais entre 104–302 ms).
Tamanho médio do evento: 443,7 bytes (N=229).

[1] `https://github.com/otavio-alv/gFHIR-HA`

8. Discussão

Os resultados obtidos indicam que a integração entre FHIR, DID/VC e evidências auditáveis *append-only* oferece um caminho viável para governança verificável de consentimento em saúde, sem impor imutabilidade ao conteúdo clínico sensível. Embora a PoC tenha sido implementada e avaliada com *ledger* em Hyperledger Fabric, os experimentos usaram dados sintéticos e ambiente controlado, sem integração com sistemas clínicos em produção ou validação em campo. Permanecem desafios como integração com sistemas legados, governança institucional, acordos de confiança interorganizacionais, escalabilidade e custo operacional.

9. Conclusão e Trabalhos Futuros

Este trabalho apresentou o gFHIR-HA, uma arquitetura híbrida para governança verificável de consentimento no compartilhamento de dados de saúde. A proposta integra interoperabilidade clínica baseada em FHIR, identidade baseada em DID/*Verifiable Credentials*, PKI regulamentada (incluindo ICP-Brasil) e uma camada *append-only* de evidências criptográficas para auditoria de eventos do ciclo de vida do consentimento.

A principal contribuição consiste na separação arquitetural entre conteúdo clínico *off-chain* e trilha de evidências auditáveis *on-chain*, conciliando interoperabilidade, auditabilidade e requisitos regulatórios associados à proteção de dados sensíveis. O trabalho também apresentou um mapeamento entre requisitos da LGPD e mecanismos técnicos da arquitetura, evidenciando como princípios de minimização, segurança e responsabilização podem ser suportados por decisões de projeto.

Como validação, implementou-se uma PoC com *ledger* em Hyperledger Fabric e eventos sintéticos, reportando métricas de latência e tamanho de evidências. Como trabalhos futuros, pretende-se ampliar a avaliação com integração a sistemas legados, análise de escalabilidade e validação em ambientes interinstitucionais reais.

Referências

Agbo, C. C., Mahmoud, Q. H., and Eklund, J. M. (2019). Blockchain technology in healthcare: a comprehensive review and directions for future research. *Applied Sciences*, 9(9):1736.

Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25–30.

Bai, P., Kumar, S., Aggarwal, G., Mahmud, M., Kaiwartya, O., and Lloret, J. (2022). Self-sovereignty identity management model for smart healthcare system. *Sensors*, 22(13):4714.

Brasil (2001). Medida provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil. Acesso em: 27 fev. 2026.

Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018 (lei geral de proteção de dados pessoais). Texto legal. Acesso em: 27 fev. 2026.

Brückner, S. et al. (2025). A user-driven consent platform for health data sharing in digital health applications. npj Digital Medicine. Acesso em: 27 fev. 2026.

El Emam, K., Jonker, E., Arbuckle, L., and Malin, B. (2011). A systematic review of re-identification attacks on health data. *PLOS ONE*, 6(12):e28071.

Gordon, W. J. and Catalini, C. (2018). Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. *Computational and Structural Biotechnology Journal*, 16:224–230.

HL7 International (2019). FHIR Release 4 (v4.0.1). Acesso em: 27 fev. 2026.

HL7 International (2026). FHIR Consent Resource. FHIR build documentation. Acesso em: 27 fev. 2026.

ITI (2008). DOC-ICP-15: Assinaturas digitais na ICP-Brasil. Normativo / documento de referência. Acesso em: 27 fev. 2026.

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Stanford, CA.

Rose, S., Borchert, O., Mitchell, S., and Connelly, S. (2020). Zero Trust Architecture. Technical Report SP 800-207, National Institute of Standards and Technology (NIST).

Voronov, A., Jafari, M., Zhao, L., Soliz, M., Hong, Q., Pope, J., Chern, D., Lipman, M., and Grando, A. (2024). Pediatric consent on FHIR. *Applied Clinical Informatics*, 15(2):342–356.

W3C (2022). Decentralized Identifiers (DIDs) v1.0. W3C Recommendation. Acesso em: 27 fev. 2026.

W3C (2025). Verifiable Credentials Data Model v2.0. W3C Recommendation. 15 May 2025. Acesso em: 27 fev. 2026.

Zhang, P., White, J., Schmidt, D. C., Lenz, G., and Rosenbloom, S. T. (2018). FHIRChain: Applying blockchain to securely and scalably share clinical data. *Computational and Structural Biotechnology Journal*, 16:267–278.