Capítulo 5

A Cadeia de Confiança na Saúde Digital: o grande desafio da interoperabilidade

Cristiano André da Costa, Priscila Schmidt Lora, André Luís del Mestre Martins, Fausto Neri da Silva Vanin, Alex Roehrs, Rodrigo da Rosa Righi, Rodolfo Stoffel Antunes

Abstract

Interoperability remains a critical barrier to the advancement of Digital Health in Brazil. Yet, simply enabling data exchange is not enough. The true challenge lies in establishing a chain of trust that guarantees both seamless information flow and patient sovereignty over their data, in full compliance with Brazil's General Data Protection Law (LGPD). Today, consent management is fragmented, opaque, and lacks granularity, eroding patient trust and engagement. This paper frames auditable, patient-centric consent as a core socio-technical challenge for healthcare computing. We introduce a conceptual model, inspired by the INTEROPCHAIN platform, that leverages blockchain technology to create an immutable, transparent consent ledger decoupled from traditional electronic health record systems. We argue that addressing this challenge will unlock an ecosystem for safer, more personalized AI applications, ultimately transforming patients from passive data subjects into active agents in their own healthcare journey.

Resumo

A interoperabilidade permanece uma das barreiras mais críticas à evolução da Saúde Digital no Brasil. Contudo, a simples troca de dados entre sistemas é insuficiente. O verdadeiro grande desafio reside na construção de uma cadeia de confiança que garanta não apenas a fluidez da informação, mas também a soberania do paciente sobre seus próprios dados, em conformidade com a LGPD. Atualmente, a gestão do consentimento é fragmentada, opaca e raramente granular, o que mina a confiança e o engajamento do cidadão. Este

artigo posiciona a interoperabilidade com a gestão de consentimento auditável como um desafio sociotécnico central para a computação aplicada à saúde. Apresentamos um modelo conceitual, inspirado nos princípios da plataforma INTEROPCHAIN, que utiliza blockchain para criar um registro imutável e transparente do consentimento, desacoplando-o dos sistemas de prontuários. Argumentamos que, ao resolver este desafio, habilitamos um ecossistema para o desenvolvimento de aplicações de IA mais seguras e personalizadas, transformando o paciente de um mero sujeito de dados em um agente ativo em sua jornada de cuidado.

5.1 Introdução

A organização do Sistema Único de Saúde (SUS) brasileiro pressupõe um cuidado integral, universal e longitudinal, em que a jornada do paciente flui de forma coordenada entre os diferentes níveis de atenção. No entanto, a materialização dessa visão enfrenta um obstáculo crônico e sistêmico: a profunda fragmentação dos dados de saúde. Na prática, o histórico clínico de um cidadão encontra-se disperso em silos de dados isolados em hospitais, clínicas e laboratórios. Este cenário não apenas compromete a continuidade do cuidado e a segurança do paciente, especialmente nas transições, como também cria um paradoxo acentuado pela Lei Geral de Proteção de Dados Pessoais (LGPD), que, legalmente, posiciona o paciente como titular soberano de suas informações.

Essa realidade nos coloca diante do que chamamos de falso dilema: de um lado, há o imperativo clínico e científico de compartilhar dados para viabilizar o cuidado coordenado, a pesquisa avançada e o desenvolvimento de inteligência artificial em saúde; do outro, há o imperativo ético e legal de garantir a privacidade e a segurança, em estrita conformidade com a LGPD (Fernandes et al., 2022). A abordagem atual impõe uma escolha precária entre esses dois polos, tratando o compartilhamento e a proteção como objetivos mutuamente excludentes.

Outro ponto crítico relacionado ao compartilhamento de registros de saúde é a diversidade estrutural desses registros. Ao longo dos anos, os registros de atendimento migraram do papel para os sistemas de informação, mas pouco se discute sobre a falta de padronização das informações. Para resolver essa questão, uma das iniciativas mais exitosas tem sido a estruturação proposta por um grupo de pesquisadores, chamado *Health Level Seven* (HL7). A partir dessa estrutura, é possível organizar os registros clínicos em blocos ou recursos, que seccionam as informações. Também como uma evolução desse padrão, atualmente esses recursos são apresentados no formato FHIR (*Fast Health Interoperability Resources*), um conjunto de recursos e interfaces de programação de aplicativos (APIs) REST baseadas em HTTP (Homback, 2025). Com isso, objetiva-se obter uma forma rápida e estruturada de compartilhamento.

Este artigo argumenta que o grande desafio da interoperabilidade não é meramente técnico, um problema a ser resolvido apenas com a adoção de padrões como o HL7 FHIR, mas, fundamentalmente, de governança e confiança. Defendemos que a interoperabilidade só alcançará seu potencial transformador quando for construída sobre uma pedra angular inegociável: uma base de consentimento explícito, granular e auditável, gerenciada ativamente pelo próprio paciente. Em síntese, é necessário

qualificar o compartilhamento de dados para que ele não apenas cumpra os pressupostos legais, mas também estabeleça uma relação de confiança que empodere o cidadão. Ao longo deste trabalho, decompomos a natureza multidimensional deste desafio e apresentamos um modelo arquitetural que visa construir a Cadeia de Confiança necessária à saúde digital no Brasil.

5.2 A Natureza Multidimensional do Desafio

A superação da barreira da interoperabilidade na saúde digital transcende a mera implementação de um padrão tecnológico. Trata-se de um desafio sociotécnico complexo, que deve ser compreendido em suas múltiplas dimensões interdependentes. A falha em endereçar qualquer uma dessas facetas resulta em uma solução incompleta, que pode até mesmo agravar problemas de confiança e de usabilidade. A seguir, decompomos este grande desafio em três eixos principais: o técnico-semântico, o ético-governamental e o da interação humano-computador.

5.2.1 Desafio Técnico e Semântico

O primeiro e mais evidente obstáculo é de natureza técnica. A adoção de padrões como o HL7 FHIR é um passo fundamental, proporcionando uma língua franca para a representação e a troca de dados de saúde. Contudo, a existência de um padrão não garante sua adoção universal ou correta. O ecossistema de saúde brasileiro é um ambiente heterogêneo (brownfield), composto por uma miríade de sistemas legados que não foram projetados para se comunicarem entre si. A modernização ou a integração desses sistemas impõe custos e complexidade significativos.

Além da barreira sintática, reside o desafio semântico: garantir que a informação seja interpretada com o mesmo significado em diferentes sistemas e contextos clínicos (Roehrs et al., 2018). A ambiguidade de terminologia, a ausência de mapeamentos consistentes entre vocabulários (como CID-10 e SNOMED CT) e a perda de contexto clínico durante a transmissão de dados podem levar a erros de interpretação com graves consequências para o cuidado do paciente. Portanto, a interoperabilidade técnica é uma condição necessária, mas não suficiente; deve ser acompanhada de rigoroso alinhamento semântico para que a troca de dados seja segura e eficaz.

5.2.2 Desafio de Governança e Ética

Se o desafio técnico questiona como os dados podem ser trocados, o desafio de governança e ética pergunta sob quais regras devem ser enviados. Este é o cerne da confiança. A LGPD estabelece o consentimento do titular como a principal base legal para o tratamento de dados pessoais, mas a sua gestão no ecossistema atual é falha. O consentimento é frequentemente coletado em formulários de papel ou em termos de serviços digitais genéricos, o que torna difícil gerenciar, granularizar ou revogar.

Este cenário levanta questões críticas: como gerenciar dinamicamente e de forma auditável o ciclo de vida completo do consentimento (concessão, revogação e expiração)? Quem é o verdadeiro custodiante do consentimento? Nos modelos atuais, a instituição que detém o dado (o custodiante do dado) também controla o consentimento, criando um conflito de interesses. Uma governança robusta exige a separação dessas responsabilidades. Adicionalmente, como garantir uma auditoria isenta e à prova de

adulteração sobre quem acessou quais dados e quando? Sem um mecanismo de auditoria transparente e confiável, a conformidade com a LGPD não se torna uma questão de fato verificável.

5.2.3 Desafio de Usabilidade e Interação Humano-Computador (HCI)

Finalmente, mesmo a arquitetura técnica e de governança mais perfeita falhará se não for acessível e utilizável pelos principais atores: pacientes e profissionais de saúde. Este é o desafio da "última milha" da interoperabilidade.

Do ponto de vista do paciente, a gestão de permissões de acesso a dados de saúde é uma tarefa complexa e sensível. A interface para essa gestão deve ser intuitiva, transparente e empoderadora, especialmente para populações com diferentes níveis de literacia digital, como os idosos. Apresentar ao cidadão comum uma longa lista de checkboxes técnicos ou de termos jurídicos constitui uma barreira que mina o engajamento e a própria noção de consentimento informado. A interface deve traduzir políticas complexas em ações simples e compreensíveis.

Do lado do profissional de saúde, qualquer sistema que introduza atrito ou adicione passos a um fluxo de trabalho já sobrecarregado está fadado à rejeição. A solicitação e o consumo de dados interoperados devem ser integrados de forma fluida e quase invisível aos sistemas de prontuário eletrônico existentes, agregando valor claro e imediato ao processo de tomada de decisão clínica. O desafio de HCI é, portanto, projetar a mediação que constrói a confiança e a eficiência, tornando a gestão da interoperabilidade e do consentimento uma ferramenta facilitadora, e não um fardo adicional.

5.3 Um Modelo Arquitetural para a Cadeia de Confiança (Baseado no INTEROPCHAIN)

Para endereçar o desafio, foi montada uma Rede de Colaboração em Saúde Digital junto à RNP (Rede Brasileira para Educação e Pesquisa). A rede congrega pesquisadores de diversas instituições brasileiras, com foco na interoperabilidade de dados estruturados e na gestão de consentimento transparente e seguro. Nesse âmbito, a rede de colaboração vem propondo o INTEROPCHAIN, um modelo arquitetural para a Cadeia de Confiança na saúde digital (Figura 1). Esse modelo é resultado da evolução de arquiteturas baseadas em blockchain propostas por pesquisadores da Rede de Colaboração (Vanin et al., 2022; da Silva Vanin, 2025; Roehrs, 2021; Roehrs, 2018; Roehrs, 2017).

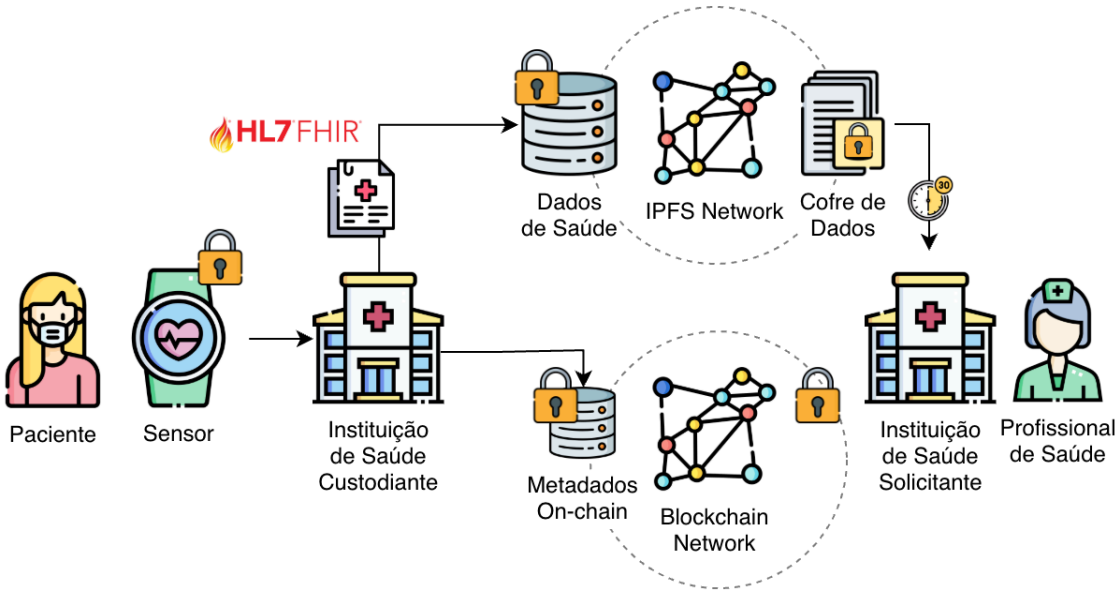

Figura 1. Visão Geral do Modelo INTEROPCHAIN

O princípio central que fundamenta o modelo arquitetural é o desacoplamento radical entre a camada de governança e consentimento e a camada de armazenamento e processamento de dados. Nos modelos tradicionais, a autorização de acesso (o consentimento) é uma propriedade intrínseca e atrelada ao sistema que armazena o dado (o prontuário eletrônico). Isso cria uma dependência rígida, aprisiona o controle do paciente em silos institucionais e torna a auditoria entre diferentes organizações um processo complexo e pouco confiável.

A proposta INTEROPCHAIN inverte essa lógica. O consentimento passa a ser um ativo digital soberano, gerenciado pelo paciente em uma infraestrutura neutra e agnóstica aos sistemas de saúde — o ledger de blockchain. Os sistemas de saúde (hospitais, clínicas, laboratórios) tornam-se consumidores dessas regras de consentimento, consultando a blockchain para verificar se têm permissão para acessar um dado específico antes de efetivamente acessá-lo no local de origem.

Esse desacoplamento é a chave para a verdadeira interoperabilidade centrada no paciente, pois transforma a permissão de acesso, um atributo local e estático, em uma política global, dinâmica e auditável.

O modelo central do INTEROPCHAIN é constituído de três componentes principais:

- **Componente 1 - O Controle de Consentimento (Blockchain):** utiliza a imutabilidade e a transparência da blockchain para registrar as regras de consentimento ("quem", "o quê", "por quanto tempo", "para qual finalidade") como *smart contracts*. Isso cria uma fonte única e auditável da verdade;
- **Componente 2: O Padrão de Dados (APIs FHIR):** Utilizar FHIR como a linguagem comum para a troca de dados, garantindo a interoperabilidade técnica e semântica;

- **Componente 3: O Cofre de Dados (Armazenamento Híbrido):** Manter os dados sensíveis de saúde armazenados de forma segura (off-chain), enquanto os metadados, os hashes de integridade e os registros de consentimento são gerenciados na blockchain (on-chain).

5.3.1 Controle ole de Consentimento

Para endereçar a ausência de uma fonte de verdade única, neutra e auditável para a gestão do consentimento, propomos um ledger distribuído, baseado em tecnologia blockchain, como a espinha dorsal da nossa arquitetura. Este componente atua como um cartório digital, cujo propósito exclusivo é registrar, validar e tornar inalteráveis as permissões de acesso aos dados de saúde, colocando o controle nas mãos do paciente.

É fundamental destacar que este ledger, em si, não armazena dados sensíveis de saúde. Essa distinção é crucial para garantir a privacidade e a escalabilidade do sistema. Em vez disso, a blockchain registra um conjunto mínimo de informações essenciais:

- A Prova do Consentimento: O registro imutável da autorização concedida pelo paciente;
- As Regras de Acesso: Os termos granulares da permissão, definindo "quem" (provedor/instituição), “o quê” (tipo de dado, como exames de imagem), "por quanto tempo" (período de validade) e "para qual finalidade" (como diagnóstico clínico ou pesquisa anônima);
- A Prova de Integridade dos Dados: Hashes criptográficos dos dados de saúde, que permitem verificar se a informação não foi alterada, sem revelar seu conteúdo;
- O Rastro de Auditoria: Um registro de todas as solicitações de acesso e de transações relacionadas ao consentimento.

Essas regras são implementadas por meio de smart contracts (contratos inteligentes), que são programas autoexecutáveis que definem e aplicam, de forma programática e determinística, os termos do consentimento. Quando um profissional de saúde solicita acesso, o sistema consulta o smart contract correspondente na blockchain, que verifica automaticamente se as condições da solicitação são válidas conforme as regras estabelecidas pelo paciente.

A natureza imutável da blockchain garante que, uma vez registrado, um consentimento (ou sua revogação) não pode ser alterado ou apagado retroativamente por qualquer das partes, seja o paciente, o hospital ou um desenvolvedor de software. Isso cria um rastro de auditoria transparente e inquestionável, empoderando o paciente com a capacidade de monitorar exatamente quem acessou suas informações e quando, e fornecendo uma base sólida para a conformidade regulatória com a LGPD.

5.3.2 O Padrão de Dados

O modelo arquitetural do INTEROPCHAIN envolve múltiplos atores trocando dados de saúde em um ambiente distribuído (por exemplo, sensores, instituições

custodiantes e solicitantes, conforme ilustrado na Figura 1). Nesse contexto, a eficácia da arquitetura baseada em blockchain para gestão do consentimento depende diretamente da capacidade de diferentes sistemas interpretarem de forma consistente os dados compartilhados. Assim, a interoperabilidade torna-se um requisito técnico obrigatório e de governança, uma vez que a aplicação adequada das políticas de consentimento depende de uma interpretação inequívoca das informações clínicas.

O FHIR organiza os registros eletrônicos de saúde por meio de estruturas padronizadas em formatos extensíveis como JSON e XML, chamados de "recursos". Todos os recursos são compostos por variados campos a serem preenchidos, mas apenas um é obrigatório: o "Tipo de Recurso". Além da interoperabilidade sintática e semântica, o padrão FHIR permite customizações para usos específicos por meio de perfis. No cenário brasileiro, por exemplo, a Rede Nacional de Dados de Saúde (RNDS) utiliza perfis do FHIR para estabelecer modelos informacionais e computacionais de integração ao ecossistema do SUS.

A troca de recursos FHIR ocorre predominantemente por meio de requisições HTTP baseadas no estilo arquitetural RESTful, podendo também incorporar mecanismos orientados a eventos conforme as necessidades de integração. Nesse cenário, a padronização promovida pelo FHIR é essencial para garantir que as políticas de consentimento registradas na blockchain sejam corretamente interpretadas e aplicadas pelos sistemas participantes. Além disso, o FHIR atua como um componente estruturante da arquitetura, viabilizando a interoperabilidade técnica, semântica e regulatória necessária à implementação da Cadeia de Confiança proposta.

5.3.3 O Cofre de Dados

A abordagem de ledger de consentimento seria inviável e insegura se os dados clínicos sensíveis fossem armazenados diretamente na blockchain. O armazenamento *on-chain* de grandes volumes de dados, como prontuários completos ou imagens médicas, é computacionalmente custoso, degrada o desempenho da rede e, mais criticamente, cria um risco perpétuo à privacidade; mesmo dados criptografados podem se tornar vulneráveis a ataques futuros à medida que a computação avança.

Para mitigar esses riscos, nosso modelo adota uma estratégia de armazenamento híbrido, materializada no conceito de Cofre de Dados (Data Vault). Este cofre é uma camada de armazenamento segura e distribuída, operando completamente *off-chain*, projetada para armazenar o conteúdo completo dos prontuários (em formato FHIR), exames de imagem e séries temporais de biossinais. Crucialmente, todos os dados no cofre são mantidos em formato criptografado, garantindo a confidencialidade em repouso.

A ligação entre o ledger de consentimento (*on-chain*) e o Cofre de Dados (*off-chain*) é estabelecida por meio de ponteiros imutáveis. Em vez de armazenar o dado em si, o *smart contract* na blockchain armazena um ponteiro para ele — tipicamente um hash criptográfico gerado por um sistema de arquivos distribuído como o InterPlanetary File System (IPFS). Este ponteiro funciona como um endereço único e à prova de violação para o dado criptografado no cofre.

Na prática, o fluxo de acesso ocorre da seguinte forma:

1. O sistema requisitante (ex.: o prontuário de um médico) valida a permissão no *smart contract* da blockchain.
2. Uma vez autorizado, ele recebe o ponteiro criptográfico do dado relevante.
3. Com este ponteiro, ele acessa o Cofre de Dados para recuperar o pacote de dados criptografados. A chave para descriptografar esses dados é gerenciada por um mecanismo seguro e separado, fora do escopo da blockchain.

A custódia dos dados no cofre permanece sob a responsabilidade de entidades confiáveis, como a instituição de saúde que mantém os dados (o *Data Steward*), garantindo a conformidade com as regulações de soberania de dados.

Essa arquitetura de Cofre de Dados resolve o paradoxo central entre interoperabilidade e privacidade: ela aproveita a governança descentralizada e a auditabilidade da blockchain para gerenciar o *acesso*, sem sacrificar a confidencialidade, a performance e a escalabilidade necessárias ao armazenamento de dados de saúde em larga escala.

5.4 Agenda de Pesquisa Aberta para a Comunidade (O Chamado à Ação)

O modelo arquitetural para a Cadeia de Confiança apresentado neste artigo oferece um caminho viável, mas não constitui uma solução final. Pelo contrário, ele estabelece uma fundação sobre a qual uma série de desafios de pesquisa complexos e fascinantes emerge. A construção efetiva deste ecossistema depende do engajamento e da colaboração da comunidade de Computação Aplicada à Saúde. A seguir, delineamos uma agenda de pesquisa aberta, convidando a comunidade a endereçar estas questões críticas.

5.4.1 Escalabilidade e Desempenho em Escala Nacional

A primeira e mais pragmática questão de pesquisa refere-se à viabilidade de uma solução baseada em blockchain para operar em escala massiva no SUS. Redes blockchain, especialmente as públicas, enfrentam limitações conhecidas quanto à vazão de dados (transações por segundo) e à latência de comunicação. Embora redes permissionadas (de consórcio) ofereçam desempenho superior, o desafio de gerenciar milhões de consentimentos e transações de auditoria em tempo real permanece. Nesse sentido, questões em aberto incluem:

- Quais arquiteturas de consenso e modelos de dados on-chain são mais eficientes para minimizar os custos computacionais e de armazenamento?
- Como estratégias de sharding, canais privados ou soluções de segunda camada poderiam ser aplicadas para segmentar o tráfego de transações e garantir o desempenho sem comprometer a auditoria global?
- Qual o impacto real da latência da rede na experiência do usuário em cenários clínicos de alta criticidade?
- Como estratégias de compressão de dados, balanceamento de carga, comunicação assíncrona e elasticidade de recursos poderiam ser incorporadas na solução em prol de garantir uma qualidade de serviço aceitável à medida que a escala de uso do sistema aumenta?

5.4.2 Interfaces Inteligentes para a Gestão de Consentimento

A soberania do paciente sobre seus dados só é efetiva se as ferramentas para exercer esse controle forem intuitivas e acessíveis. Delegar ao cidadão comum a tarefa de definir políticas de acesso granulares por meio de formulários complexos constitui uma barreira intransponível. O desafio aqui é usar a Inteligência Artificial para servir como uma mediadora inteligente. A pesquisa deve focar em:

- O desenvolvimento de interfaces conversacionais ou baseadas em Processamento de Linguagem Natural (PLN) que permitam ao paciente expressar suas preferências de compartilhamento em linguagem cotidiana (ex.: "permitir que cardiologistas vejam meus exames de coração dos últimos dois anos");
- A criação de algoritmos de IA capazes de traduzir essas instruções em regras formais e inequívocas para os smart contracts na blockchain;
- O projeto de mecanismos de feedback e validação que garantam ao paciente a compreensão e a confirmação da política gerada, mitigando riscos de interpretação ambígua pela IA.

5.4.3 A Fronteira da Análise de Dados com Privacidade

A Cadeia de Confiança habilita o acesso consentido a dados distribuídos, criando uma oportunidade sem precedentes para o treinamento de modelos de IA. No entanto, o desafio é realizar essa análise sem centralizar os dados nem expô-los em sua forma bruta. Esta é a fronteira da análise de dados com privacidade (privacy-preserving analytics). A comunidade deve explorar:

O aprendizado federado vem se destacando como a principal alternativa para o treinamento de modelos de aprendizado de máquina em repositórios de dados distribuídos que não podem ser compartilhados livremente. O aprendizado federado considera o compartilhamento de algoritmos de treinamento e de parâmetros atualizados e anonimizados, evitando que dados sensíveis de pacientes sejam colocados em risco. Esta abordagem vem sendo amplamente estudada no meio acadêmico e alinha-se perfeitamente à natureza distribuída da solução proposta neste artigo.

A viabilidade da Criptografia Totalmente Homomórfica (FHE), que permite realizar cálculos diretamente sobre dados criptografados. Embora ainda computacionalmente intensiva, a FHE representa a fronteira futura para análises complexas, e a pesquisa sobre sua aplicação em cenários clínicos específicos é de vital importância.

5.4.4 Modelos de Negócio e Sustentabilidade

Por fim, nenhuma inovação tecnológica sobrevive sem um modelo de sustentabilidade viável. Uma infraestrutura de confiança neutra, que não pertence a nenhuma instituição de saúde específica, requer um modelo de governança e de custeio claros. As questões de pesquisa nesta área são socioeconômicas e cruciais:

- Qual o modelo de governança mais adequado para essa infraestrutura? Seria um bem público digital mantido pelo Estado, um consórcio de instituições de saúde ou uma fundação independente?
- Como financiar a operação e a manutenção da rede de forma equitativa e sustentável em nível nacional?

- Quais incentivos (regulatórios, financeiros ou operacionais) podem ser criados para estimular a adesão de hospitais, clínicas, laboratórios e desenvolvedores de software a este ecossistema de confiança?

5.5. Conclusão

A interoperabilidade de dados de saúde, quando concebida exclusivamente como um problema de padronização técnica e de troca sintática de informações, constitui uma solução incompleta para os desafios da Saúde Digital no Brasil. A adoção de padrões como o HL7 FHIR e a expansão de iniciativas como a RNDS representam avanços necessários, porém insuficientes. Sem uma camada de governança que assegure ao paciente o controle efetivo sobre quem acessa seus dados, em quais condições e para qual finalidade, a integração entre sistemas permanece desprovida do elemento que lhe confere legitimidade: a confiança.

O modelo arquitetural proposto neste artigo utiliza um ledger distribuído para viabilizar o desacoplamento entre a gestão do consentimento e os sistemas de armazenamento de dados clínicos. Portanto, a proposta oferece um caminho concreto para a construção da cadeia de confiança entre pacientes e repositórios de dados. Ao registrar as regras de consentimento de forma imutável, granular e auditável, e ao manter os dados sensíveis em cofres criptografados off-chain, a arquitetura proposta atende simultaneamente aos requisitos de interoperabilidade, privacidade e conformidade com a LGPD, sem impor a escolha entre compartilhamento e proteção dos dados.

Essa base de confiança torna possível conceber um ecossistema de saúde digital no qual o fluxo de dados não ocorre à revelia do cidadão, mas sim é viabilizado por sua participação ativa e informada. Nesse ecossistema, o consentimento deixa de ser um formulário genérico assinado uma única vez e passa a constituir um ativo digital soberano, por meio do qual o paciente define, de forma granular e dinâmica, as condições de acesso às suas informações clínicas. Essa capacidade de gestão ativa, aliada a um rastro de auditoria que permite verificar exatamente quem acessou seus dados e quando, transforma a posição do paciente no ecossistema de mero sujeito passivo de coleta em agente com capacidade decisória. Essa inversão de lógica habilita o desenvolvimento de aplicações de Inteligência Artificial mais seguras e personalizadas, operando sobre dados cuja proveniência, integridade e autorização de uso são verificáveis de ponta a ponta.

Portanto, a construção de um ecossistema de saúde digital verdadeiramente interoperável, seguro e centrado no paciente não é uma empreitada de uma única instituição ou grupo de pesquisa, mas sim um desafio nacional que exige a convergência de esforços. Este artigo apresentou um modelo arquitetural e uma agenda de pesquisa, mas são apenas os primeiros passos de uma longa jornada. Convidamos, assim, a comunidade de computação aplicada à saúde, juntamente com gestores, profissionais clínicos, formuladores de políticas e, principalmente, cidadãos, a colaborar ativamente na construção e no aprimoramento desta Cadeia de Confiança. É somente por meio de uma aliança multidisciplinar e de um compromisso compartilhado com a soberania do

paciente que poderemos transformar a promessa da saúde digital em uma realidade tangível e confiável para todos os brasileiros.

Agradecimentos

Os autores gostariam de agradecer à RNP (Rede Brasileira para Educação e Pesquisa) pelo financiamento do projeto INTEROPCHAIN, por meio do Programa de Redes de Colaboração em Saúde Digital (PRC-SD).

Referências

da Silva Vanin, F. N., Melo, B., da Rosa Righi, R., da Costa, C. A., & Antunes, R. S. (2025). Enhancing Health Data Integrity Through On-Chain Verification and Cryptographic Proofs. *Blockchain: Research and Applications*, 100373.

Fernandes, M. E., & Nuzzi, A. P. E. (2022). Fundamentos da Lei Geral de Proteção de Dados (LGPD): uma revisão narrativa. Research, Society and Development, 11(12), e310111234247-e310111234247.

Hornback, A., Marteau, B., Tan, S. Q., Kim, K., Patil, O., Traynelis, J., ... & Wang, M. D. (2025). FHIR in Focus: Enabling Biomedical Data Harmonization for Intelligent Healthcare Systems. IEEE Reviews in Biomedical Engineering.

Roehrs, A., Da Costa, C. A., & da Rosa Righi, R. (2017). OmniPHR: A distributed architecture model to integrate personal health records. *Journal of biomedical informatics*, *71*, 70-81.

Roehrs, A., da Costa, C. A., da Rosa Righi, R., Rigo, S. J., & Wichman, M. H. (2018). Toward a model for personal health record interoperability. *IEEE journal of biomedical and health informatics*, *23*(2), 867-873.

Roehrs, A., da Costa, C. A., Righi, R. R., Mayer, A. H., da Silva, V. F., Goldim, J. R., & Schmidt, D. C. (2021). Integrating multiple blockchains to support distributed personal health records. *Health Informatics Journal*, *27*(2), 14604582211007546.

Vanin, F. N. D. S., Policarpo, L. M., Righi, R. D. R., Heck, S. M., da Silva, V. F., Goldim, J., & da Costa, C. A. (2022). A blockchain-based end-to-end data protection model for personal health records sharing: a fully homomorphic encryption approach. *Sensors*, *23*(1), 14.

Sobre os Autores

Prof. Dr. Cristiano André da Costa é Professor Titular da Unisinos e Diretor do SOFTWARELAB, núcleo de inovação em software. Atua nas áreas de Sistemas Distribuídos, Inteligência Artificial e Saúde Digital, com foco em ecossistemas de saúde inteligentes e interoperáveis utilizando tecnologias como Blockchain e Internet das Coisas. Foi reconhecido como Pesquisador Gaúcho em Ciência da Computação e Informação pela Fapergs em 2025. É bolsista de produtividade do CNPq e membro sênior da IEEE e da ACM. Coordenou a Comissão Especial de Computação Aplicada à Saúde da SBC (23~25) e possui mais de 10.000 citações de suas publicações científicas.

Profa. Dra. Priscila Lora é Professora e Líder de Pesquisa na Unisinos. Doutora (2013) e Mestre (2009) em Ciências Médicas pela Ufrgs, especialista em Análises Clínicas pela Ufrgs e farmacêutica bioquímica formada pela Pontifícia Universidade Católica do Rio Grande do Sul. Possui experiência em gestão de projetos e captação de recursos para pesquisa e desenvolvimento de produtos e tecnologias, além de atuação na transferência de conhecimento no contexto da interação universidade-indústria no Brasil. Seus interesses de pesquisa incluem o desenvolvimento de biossensores para diagnóstico de doenças, com foco na detecção de biomarcadores, e tecnologias de saúde digital.

Prof. Dr. André Luís del Mestre Martins é Professor Titular do IFSul. Possui experiência em projetos de extensão tecnológica para transformação digital dos serviços de saúde em parceria com o Hospital Regional de São Jerônimo. Seus interesses de pesquisa incluem Informática em Saúde, interoperabilidade, e IoT aplicada à saúde.

Dr. Fausto Neri da Silva Vanin é bolsista Capes de pós-doutorado no Programa de Pós-Graduação em Computação Aplicada da Unisinos. É sócio da OnePercent, empresa que desenvolve soluções com tecnologias blockchain desde 2017. É também pesquisador do Auto-id Lab do KAIST, Coreia do Sul. Sua tese recebeu o Prêmio Artur Ziviani no Simpósio Brasileiro de Computação Aplicada à Saúde de 2025.

Prof. Dr. Alex Roehrs é professor colaborador do PPGCA da Unisinos, pesquisador vinculado ao VIZLAB e ao SOFTWARELAB, atua na docência, na pesquisa e na gestão acadêmica, incluindo a coordenação da Especialização em Inteligência Artificial Aplicada. Doutor e Mestre em Computação Aplicada, trabalha com Engenharia de Software, Arquitetura de Sistemas, Blockchain, IoT e saúde digital, com produção científica e projetos em cooperação nacional e internacional. Também possui mais de 25 anos de experiência profissional em tecnologia, projetos e arquitetura de sistemas.

Prof. Dr. Rodrigo da Rosa Righi é membro sênior da IEEE e da ACM, e bolsista de produtividade do CNPq há 9 anos. Também é coordenador do Programa de Pós-Graduação em Computação Aplicada da Unisinos. Possui pós-doutorado, realizado no KAIST - Coreia do Sul, com ênfase nas áreas de IoT e Cloud Computing. Faz parte do Comitê de Assessoramento da FAPERGS. Prof. Rodrigo possui uma produção acadêmica crescente, com Google H-Index de 43 e i10-index de 111 (03/2026).

Prof. Dr. Rodolfo Stoffel Antunes é professor assistente da Unisinos e Pesquisador no Programa de Pós-Graduação em Computação Aplicada. Realizou Pós-Doutorado em Computação na Friedrich-Alexander-Universität Erlangen-Nürnberg na Alemanha. Pesquisador vinculado ao SOFTWARELAB. Atua no desenvolvimento de projetos de pesquisa em computação aplicada em parceria com empresas, com foco no desenvolvimento de produtos de software para a área da Saúde e IoT. Seus interesses de pesquisa incluem a aplicação de IoT, Redes Orientadas a Conteúdo, Sistemas Distribuídos e Computação Móvel e Ubíqua.

