Digital Prescription and Dispensation of Medications

Liverson Paulo Furtado Severo
Jean Everson Martina
liverson.p@posgrad.ufsc.br
jean.martina@ufsc.br
Universidade Federal de Santa Catarina
Florianópolis, Santa Catarina, Brasil

Abstract

Context: In Brazil, the prescription and dispensing of medications remain largely manual, relying on physical documents. This approach poses challenges for security, traceability, and regulatory compliance, especially for controlled substances.

Problem: Manual systems are insufficient for tracking medication dispensing, preventing misuse, and ensuring interoperability between healthcare providers and pharmacies.

Solution: This study proposes a system that integrates the FHIR interoperability standard, adapted to produce self-contained documents, with JAdES digital signatures for secure and authentic prescription records. Blockchain is used to enable traceability and control over medication dispensing through an immutable record of transactions.

Method: The research employed a Proof of Concept (PoC) methodology to validate the proposed system, focusing on analyzing the current manual processes and proposing a digital solution to address identified gaps. This PoC was conducted in a controlled laboratory environment to simulate real-world scenarios and test the integration of FHIR, JAdES signatures, and Blockchain technologies to evaluate the system's functionality and compliance with regulatory requirements.

Results: The system successfully generated secure, self-contained digital prescriptions and used Blockchain to trace and control medication dispensing. It improved regulatory compliance and addressed interoperability issues by eliminating external dependencies.

Contributions: This work advances healthcare information systems by combining interoperability standards, electronic signatures, and Blockchain to digitize and secure critical processes, addressing key challenges in medication management.

CCS Concepts

• **Applied computing** → **E-government**; • **Information systems** → **Distributed storage**; • **Human-centered computing** → **Collaborative and social computing devices**; • **Social and professional topics** → **Health information exchanges**.

Keywords

JSON, JWS, FHIR, JAdES, signature, Blockchain, interoperability

1 Introdução

A pandemia de COVID-19 acelerou significativamente a adoção de documentos médicos digitais no Brasil e no mundo, impulsionando a necessidade de soluções seguras para prescrição e dispensação eletrônica de medicamentos [4]. No país, a legislação já permite a emissão de documentos médicos eletrônicos com validade jurídica, desde que assinados digitalmente. Em especial, a Lei nº 14.063/2020 estabelece a obrigatoriedade de assinaturas qualificadas para receituários de controle especial e atestados médicos [19].

Este trabalho é uma extensão e aprimoramento de uma pesquisa previamente apresentada por [21], onde foi proposta uma arquitetura inicial para prescrição e dispensação de medicamentos utilizando HL7 FHIR e assinaturas JAdES. A presente versão amplia o escopo ao incluir mecanismos de rastreabilidade baseados em Blockchain e aprofunda a discussão sobre a interoperabilidade com o sistema brasileiro de saúde.

Apesar desse avanço, a interoperabilidade entre os diferentes sistemas de saúde ainda representa um desafio. A Rede Nacional de Dados em Saúde (RNDS) [13] busca padronizar essa troca de informações, mas a implementação e adoção dos padrões ocorre de forma lenta [20]. Atualmente, a prescrição de medicamentos no Brasil ocorre, em sua maioria, por meio de documentos físicos, o que dificulta o controle da dispensação, a rastreabilidade e a prevenção de fraudes.

Com o propósito de definir uma padronização de informações na área da saúde do Brasil, o projeto RNDS adota o padrão Fast Healthcare Interoperability Resources (FHIR), desenvolvido pela Health Level Seven International (HL7), como base para padronizar o intercâmbio de informações médicas. No entanto, este modelo precisa passar por uma adequação para uso como documento digital válido, suas informações devem ser autocontidas, ou seja, não podem depender de referências externas que possam se modificar com o tempo. Como o formato original do HL7 FHIR utiliza hiperlinks para armazenar informações sobre pacientes e prescrições, é necessário adaptá-lo para garantir a integridade dos dados ao longo do tempo.

Outro fator crítico na digitalização da prescrição de medicamentos é a necessidade de garantir autenticidade e validade jurídica dos documentos assinados eletronicamente. No Brasil, as assinaturas digitais seguem diferentes classificações, sendo que as assinaturas qualificadas são exigidas para determinados documentos médicos [19]]. Entre as abordagens existentes, o padrão JAdES (JSON Advanced Electronic Signatures) se destaca como uma alternativa robusta para a autenticação de documentos em formato JSON, permitindo a inclusão de metadados essenciais, como timestamps e informações sobre o certificado utilizado [8].

Para que a prescrição e a dispensação de medicamentos ocorram de forma regulamentada no Brasil, é necessário também garantir que tanto o médico quanto o farmacêutico estejam devidamente habilitados para exercer suas funções. No caso dos médicos, a profissão é são estabelecidas diretrizes para o exercício da medicina e a obrigatoriedade de registro no Conselho Federal de Medicina (CFM)

e nos Conselhos Regionais de Medicina (CRMs) para garantir a legalidade da prática médica [17].

Já os farmacêuticos, responsáveis pela dispensação dos medicamentos prescritos, devem cumprir os requisitos estabelecidos pela Lei nº 3.820/1960, que regula a profissão farmacêutica e determina a necessidade de registro no Conselho Federal de Farmácia (CFF) e nos Conselhos Regionais de Farmácia (CRFs) [18]. Dessa forma, qualquer sistema digital de prescrição e dispensação deve incluir mecanismos que validem as credenciais desses profissionais, garantindo que apenas indivíduos legalmente autorizados possam realizar tais atividades.

Embora a adoção de assinaturas digitais represente um avanço, a falta de rastreabilidade e controle sobre a dispensação de medicamentos, especialmente os controlados, ainda é um problema crítico. Uma solução para isso é a integração de *Blockchain*, que possibilita o registro imutável de transações, garantindo maior segurança e controle sobre a distribuição dos medicamentos prescritos. A tecnologia *Blockchain* já é reconhecida por suas propriedades de transparência, segurança e descentralização [3].

Diante desse cenário, este trabalho propõe um modelo digital seguro para prescrição e dispensação de medicamentos, integrando três tecnologias: HL7 FHIR, para padronização e interoperabilidade; assinatura JAdES, para garantir autenticidade e validade jurídica; e *Blockchain*, para rastreabilidade e controle das dispensações. Essa abordagem expande um estudo anterior, no qual foi apresentada uma arquitetura inicial para prescrição digital baseada em FHIR e JAdES. A presente versão aprimora esse modelo, incorporando mecanismos de rastreamento baseados em *Blockchain* e aprofundando a discussão sobre interoperabilidade e segurança.

2 Tecnologias utilizadas

2.1 HL7 FHIR: Padrão para interoperabilidade na Saúde

A digitalização dos serviços de saúde exige soluções que garantam a interoperabilidade e a integridade dos dados médicos, possibilitando a troca segura de informações entre diferentes sistemas. O Fast Healthcare Interoperability Resources (FHIR), desenvolvido pela Health Level Seven International (HL7), foi projetado para padronizar essa comunicação plataformas hospitalares e demais instituições de saúde [7]. Segundo [14], o FHIR é uma solução para compartilhamento de dados de saúde com o uso de componentes modulares, no qual diversos desenvolvedores trabalham incansavelmente para contribuir para os vários componentes de especificação que podem ser utilizados em diversos contextos como de guia de boas práticas, tradução de arquitetura de documentos clínicos e cuidados clínicos de lesões.

Ao longo das últimas décadas, a HL7 desenvolveu diferentes versões de padrões para a troca de informações médicas. O HL7 V2, lançado em 1989, foi amplamente adotado por sistemas hospitalares para troca de mensagens clínicas, mas apresentava estrutura rígida e difícil interpretação humana. O HL7 V3, introduzido em 1995, trouxe um modelo mais estruturado baseado em arquitetura orientada a objetos, mas sua implementação demandava um esforço elevado de desenvolvimento, limitando sua adoção [2].

Para superar essas limitações, o HL7 FHIR foi desenvolvido em 2011, combinando os benefícios das versões anteriores com tecnologias modernas de transferência de dados. O padrão utiliza um modelo baseado em recursos modulares e permite a transmissão de dados nos formatos JSON, XML e RDF, otimizando a compatibilidade com aplicações web e móveis. Além disso, sua estrutura permite uma adoção mais ágil e escalável, sendo compatível com APIs RESTful [22].

O HL7 FHIR é dividido em dois principais componentes para organização e transmissão dos dados: recursos e perfis. Os recursos (resources) são Unidades modulares de informação estruturada, podendo representar dados clínicos, administrativos ou operacionais. São intercambiáveis nos formatos JSON e XML e transportados via HTTPS. Os perfis (profiles) são uma especialização de um recurso FHIR que define restrições, extensões e especificações adicionais para adequá-lo a necessidades particulares. Segundo [2], recursos FHIR possuem as seguintes características:

- Devem ter um limite claro, que corresponda a um ou mais escopos transação lógica;
- Devem ser diferentes em significado, não apenas em uso;
- Precisam ter identidade natural;
- Devem ser muito comuns e muito utilizados em transações comerciais;
- Não devem ser específicos ou detalhados o suficiente para impedir o suporte de uma grande escala de transações comerciais;
- Devem ser mutualmente exclusivos;
- Podem usar outros recursos, mas não pode ser apenas uma composição de recursos, precisa trazer conteúdo novo;
- Devem ser reconhecidos em um *framework* lógico baseado na semelhança do recurso e ao que ele está conectado;
- Devem ser grandes o suficiente para ter um contexto de significado.

2.2 Assinaturas Digitais JAdES

Para uma adoção de documentos digitais na área da saúde, é preciso que hajam mecanismos robustos de autenticação e segurança. Para garantir a validade jurídica e a integridade das prescrições médicas eletrônicas, a melhor abordagem é o uso de assinaturas digitais avançadas, como as definidas no padrão JSON Advanced Electronic Signatures (JAdES).

O desenvolvimento de assinaturas eletrônicas avançadas ganhou força com a regulamentação europeia sobre serviços de confiança digital, estabelecida pelo European Telecommunications Standards Institute (ETSI). Esse esforço resultou na criação da família de Assinaturas Eletrônicas Avançadas (AdES), que se consolidou como um padrão amplamente adotado para garantir autenticidade, integridade e não repúdio em documentos digitais [8].

As assinaturas digitais avançadas, conforme definido por [1] e citado por [9], devem estar diretamente vinculadas ao signatário, ser geradas a partir de dados criptográficos de uso exclusivo do titular e possuir mecanismos que detectem qualquer alteração posterior no documento assinado. Dentro desse contexto, em 2021 foi introduzido o JAdES, uma evolução das assinaturas baseadas em JSON Web Signature (JWS), definida por [11], que incorpora novos

atributos para garantir a conformidade com normas internacionais e a validade de longo prazo das assinaturas [12].

O padrão JAdES define diferentes níveis de assinatura, que são aplicados conforme a necessidade do documento assinado. Esses níveis são incrementais, ou seja, cada um adiciona novos requisitos para aumentar a segurança e validade da assinatura, esse níveis podem ser definidos da seguinte forma:

- B-B (*Baseline - Basic*): Inclui parâmetros assinados e alguns atributos opcionais não assinados, garantindo a autenticidade da assinatura.
- B-T (*Baseline - Timestamp*): Acrescenta um carimbo de tempo confiável, permitindo comprovar a existência da assinatura em um determinado momento.
- B-LT (*Baseline - Long Term*): Exige a incorporação de todos os materiais de validação (como certificados) no documento assinado, garantindo sua validade a longo prazo.
- B-LTA (*Baseline - Long Term Archive*): Introduz carimbos de tempo adicionais e verificações periódicas, assegurando que a assinatura possa ser validada mesmo após muitos anos.

A escolha do nível de assinatura depende do contexto de uso. No caso da prescrição digital, o nível B-T é recomendado, pois permite comprovar a autenticidade do documento no momento da assinatura [9]. Assim há a garantia com a conformidade conformidade com a legislação brasileira.

A assinatura JWS é divida em *JOSE header* onde são armazenados os cabeçalhos da assinatura, *payload* que contém as informações do documento assinado e *signature* que é a própria assinatura. Além disso, [11] definiu o parâmetro *algorithm* (alg), que define o algoritmo criptográfico, responsável por especificar a forma que a assinatura foi gerada como obrigatório. A Figura 1 demonstra uma assinatura JWS.

Os parâmetros *Critical* (crit), que especifica os elementos adicionais que devem ser obrigatoriamente interpretados para a validação da assinatura, *Content Type* (cty), que define o tipo de mídia contida no payload da assinatura para evitar ambiguidades na interpretação dos dados, *X.509 Certificate SHA-256 Thumbprint* (x5t#S256), responsável por armazenar o hash do certificado digital utilizado na assinatura, e *X.509 Certificate Chain* (x5c), que contém a cadeia de certificação do signatário, são parâmetros opcionais no JWS, mas tornaram-se obrigatórios no JAdES, conforme definido pelo [10].

Além dos parâmetros herdados do JWS, o JAdES introduz elementos adicionais para garantir a validade e a longevidade das assinaturas digitais. O *Claimed Signing Time* (SigT) registra o momento exato em que a assinatura foi realizada. O *X.509 Signature Certificate Digest* (x5t#o) armazena o hash dos certificados utilizados. Além disso, o parâmetro *X.509 Certificates Digests* (SigX5ts) armazena múltiplos hashes dos certificados.

2.3 Hyperledger Fabric

Uma *Blockchain* é uma lista encadeada de blocos de dados conectados com o uso de ponteiros com apontamento para o *hash* do bloco "pai" e armazenados de maneira distribuída com *peer-to-peer* (P2P), com carimbos de tempo do momento em que o bloco foi inserido na lista, onde a lista de blocos cresce de maneira incessante e é segurada com o uso de princípios de criptografia com a eliminação

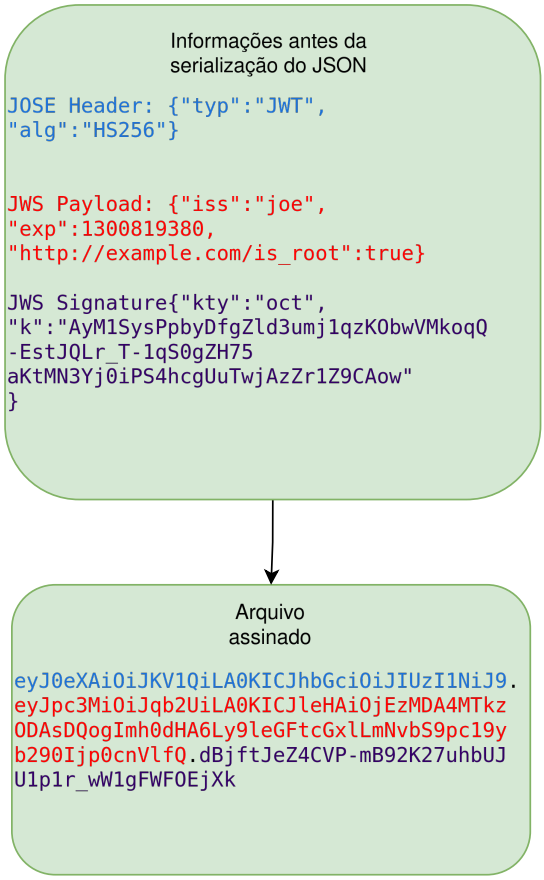

Figure 1: Exemplo de assinatura JWS. Adaptado de [11]

da necessidade de uma terceira parte para o monitoramento de transações, características de não repúdio de dados e propriedade de imutabilidade [20] e [3].

O valor *hash* de cada bloco é único e tem eficácia em prevenção de fraudes, já que a mudança mudanças em valores dentro o bloco muda imediatamente o valor do *hash* [15]. Uma vez que os blocos são conectados não podem ser modificados de forma retroativa sem a modificação dos blocos subsequentes, além disso cada *peer* na *network* possui uma cópia do livro-razão com todo o histórico de transações e o atualiza a cada nova transação. Mecanismos de consenso são utilizados para gerar, atualizar e validar transações para a garantia da segurança [3].

O *Hyperledger Fabric* é uma plataforma de *Blockchain* permissionada desenvolvida pela IBM e pela fundação Linux que serve como base para o desenvolvimento de soluções com arquitetura modular. Possui as características de confidencialidade, escalabilidade e resiliência e utiliza contratos inteligente e algoritmos de consenso que pode ser o *Crash Fault Tolerant* (CFT)ou Byzantine Fault Tolerant (BFT) [3].

3 Estado da arte

Para a construção da revisão de literatura, realizamos uma busca em bases de dados acadêmicas reconhecidas, incluindo IEEE Xplore,

ACM Digital Library e Google Scholar. A pesquisa utilizou strings de busca combinando os termos *"HL7 FHIR"*, *"prescription blockchain"* e *"digital signatures in healthcare"*. A escolha dos termos visou abranger estudos que abordassem a digitalização de documentos médicos, a utilização de assinaturas digitais, a interoperabilidade de documentos de saúde e a aplicação de *Blockchain* em contexto de saúde. A busca foi limitada a artigos publicados nos últimos cinco anos, priorizando estudos mais recentes e relevantes para o tema.

A filtragem foi realizada em quatro etapas. Na primeira etapa, os artigos foram pré-selecionados com base na ordem de relevância retornada pela base de dados, considerando fatores como citações e impacto. Na segunda etapa, foi realizada uma análise inicial dos títulos e resumos dos artigos retornados para descartar aqueles que não estavam diretamente relacionados ao tema central da pesquisa. Na terceira etapa, os artigos pré-selecionados foram submetidos a uma análise com foco na introdução e nos objetivos do estudo, para garantir que abordassem questões específicas de interoperabilidade, segurança e rastreabilidade de documentos médicos. Por fim, na quarta etapa, os artigos foram lidos de forma integral e foram selecionados aqueles que apresentavam contribuições significativas para o entendimento dos desafios e soluções propostas no contexto da prescrição e dispensação digital de medicamentos para compor o estado da arte.

O HL7 FHIR tem sido amplamente explorado para aprimorar a troca padronizada de informações médicas entre sistemas distintos. Estudos como o de [22] analisam o impacto do FHIR na interoperabilidade clínica, compilando uma revisão da literatura existente e identificando limitações na adoção do padrão em cenários médicos.

Outro trabalho relevante,[6], desenvolveu um serviço de pré-processamento para carregar dados FHIR diretamente, convertendo-os em um formato SQL otimizado para análise clínica. Essa abordagem facilita pesquisas médicas em larga escala, reduzindo a necessidade de dependência de servidores em nuvem.

A segurança dos documentos digitais é um ponto crítico no setor da saúde. Pesquisas como a de [5] investigam a aplicação de assinaturas digitais qualificadas em sistemas públicos, demonstrando ganhos na confiabilidade e redução da burocracia administrativa.

No contexto da prescrição digital, o padrão JAdES (JSON Advanced Electronic Signatures) tem sido adotado para garantir autenticidade e não repúdio dos documentos. O estudo de [8] discute como a incorporação de timestamps e certificados digitais fortalece a segurança das assinaturas em JSON, tornando o JAdES uma alternativa robusta para aplicações médicas.

A adoção de Blockchain no setor da saúde tem sido amplamente investigada para garantir a integridade e rastreamento de informações sensíveis. [3] propõe uma Blockchain permissionada para armazenar e compartilhar registros de saúde eletrônicos, permitindo a troca segura de informações entre médicos, hospitais e pacientes.

Já o trabalho de [20] desenvolve o projeto OmniPHR Multi-Blockchain, que busca otimizar a distribuição de registros médicos pessoais através de múltiplas redes descentralizadas. Essa abordagem melhora a escalabilidade sem comprometer a segurança dos dados.

Diferentemente dessas pesquisas, o modelo proposto neste estudo integra Blockchain à prescrição digital, garantindo que medicamentos controlados sejam dispensados de forma regulamentada e permitindo a rastreabilidade das transações sem comprometer a privacidade dos pacientes. Essa abordagem expande os resultados obtidos na pesquisa inicial para prescrição digital baseada em HL7 FHIR e JAdES, com a criação de um modelo autocontido que elimina a dependência de hiperlinks externos, garantindo a integridade, autenticidade e conformidade regulatória dos documentos obtidas em [21].

4 Metodologia

O desenvolvimento deste estudo seguiu uma abordagem estruturada para garantir a viabilidade técnica e a eficácia da implementação de um sistema para prescrição e dispensação digital de medicamentos. Assim, o uso do padrão HL7 FHIR para garantir a interoperabilidade entre diferentes plataformas de saúde, assinaturas JAdES para assegurar a autenticidade e validade jurídica dos documentos e *Blockchain* para a rastreabilidade e segurança no processo de dispensação formam os três pilares tecnológicos desta pesquisa.

O desenvolvimento do estudo seguiu uma abordagem estruturada para garantir a viabilidade técnica e a eficácia da implementação de um sistema com integração de um padrão de interoperabilidade para facilitar a transimssão de dados entre diferentes estabelecimentos, assinaturas digitais para a segurança dos documentos de prescrição e dispensação e *Blockchain* para realizar a rastreabilidade dos documentos de uma forma coesa e funcional, identificando possíveis limitações técnicas, a realização de ajustes iterativos e a garantia de conformidade com padrões regulatórios.

4.1 Escolha da Abordagem Metodológica

A abordagem escolhida para pesquisa foi a Prova de Conceito (PoC) para validação da viabilidade técnica do sistema antes de uma possível implementação em ambiente real. Essa abordagem foi escolhida porque permite testar a integração de tecnologias emergentes, avaliar seu funcionamento em um cenário controlado e identificar ajustes necessários antes de aplicar a solução em larga escala. O ambiente de testes foi configurado para simular interações reais entre médicos, pacientes e farmacêuticos, replicando o fluxo de prescrição e dispensação digital, para garantir a avaliação prática do sistema.

4.2 Desenvolvimento e integração das tecnologias

Para padronizar a troca de informações médicas, foi adotado o HL7 FHIR. O primeiro passo foi analisar as versões HL7 V2 e HL7 V3, que, apesar de serem padrões amplamente utilizados, apresentavam dificuldades de interpretação e integração com sistemas modernos. O HL7 FHIR, por sua vez, foi escolhido por oferecer um modelo mais flexível e modular, além de suporte nativo a JSON e XML, que são padrões com maior, o que facilita sua implementação em APIs RESTful e que possuem a viabilidade de realizar uma assinatura eletrônica de documento.

Para a decisão do padrão dentre os disponíveis, foi escolhido o JSON por apresentar um menor consumo de memória e processamento e possuir uma maior facilidade de manipulação e integração com sistemas modernos, como demonstrado na Tabela 1. Com base nesses resultados, o JSON foi definido como padrão ideal para estruturação dos documentos FHIR, garantindo eficiência no armazenamento e na troca de informações.

Table 1: Comparação JSON e XML adaptado de [16]

	JSON	XML
Número de objetos	100000	100000
Tempo total(ms) de transferência	7497.36	310017.47
Tempo médio(ms) de transferência	0.07	3.10
Uso médio de % CPU do sistema	11.30	36
Uso médio de % memória da memória	68.06	68.79

O próximo passo a ser definido foi o padrão de assinatura digital que garantiria a validação dos documentos no formato JSON. Inicialmente, a escolha natural foi o JWS, mas sua implementação apresentou dois desafios. O primeiro está relacionado à exigência de parâmetros específicos no cabeçalho para que a assinatura tenha qualificação jurídica, um requisito fundamental para prescrições médicas digitais. Diante dessa necessidade, optou-se pelo uso do JAdES, selecionando o nível mais básico capaz de atender aos requisitos legais exigidos para esse tipo de documento.

Outro desafio identificado foi a limitação do HL7 FHIR em seu formato original, que, embora seja um padrão consolidado para troca de dados médicos, não gera documentos completos e autocontidos. Isso ocorre porque o FHIR utiliza referências externas via *hiperlinks* para armazenar informações essenciais, como dados do médico, do paciente e dos medicamentos prescritos. Para viabilizar a assinatura digital e garantir a integridade dos documentos, todas as informações relevantes foram padronizadas no formato JSON e incorporadas diretamente no arquivo. Essa adaptação transforma o conteúdo em um documento independente e verificável, eliminando a necessidade de consultas a fontes externas dinâmicas.

Após a solução das adaptações necessárias o próximo ponto a ser solucionado do sistema foi relacionado à prescrição de medicamentos especiais cujo o uso é controlado. Esses medicamentos não podem ser vendidos sem uma prescrição e o projeto precisa garantir que o paciente não vai utilizar uma receita digital que já teve todos os medicamentos dispensados para comprar remédios controlados repetidas vezes.

Para isto foi definido o uso de *Blockchain* com o *Hyperledger Fabric*, assim é possível aproveitar as propriedades de imutabilidade, rastreabilidade e segurança para garantir que os remédios receitados serão comprados de maneira controlada. A arquitetura do *Fabric* segue o paradigma *executer-order-validate* com foco na resiliência, flexibilidade e confidencialidade. Este segundo [3] pode ser seguido pelas seguintes funções:

(1) Cliente realiza a submissão de propostas de execução;
(2) Pares executam as propostas de transação e validam a transação com registros de atualizações no livro-razão em formato de corrente *hash*;
(3) É formado um serviço de ordenação por ordenadores que estabelece a ordem de todas as transações do *Fabric* via protocolo de consenso;
(4) Pares endossantes validam transações contra políticas de endosso específica antes de realizar a confirmação no livro-razão.

Para viabilizar a assinatura digital no formato JAdES, foi desenvolvida uma API dedicada, responsável por implementar os parâmetros exigidos pela norma do JAdES. Os elementos necessários incluem: *Algorithm* (Alg), que especifica o algoritmo criptográfico utilizado; *Claiming Signing Time* (SigT), que registra o momento exato da assinatura; *Critical* (Crit), que indica parâmetros adicionais que devem ser processados obrigatoriamente; e um parâmetro relacionado ao certificado do signatário, que pode ser *X.509 Certificate SHA-256 Thumbprint* (X5t#S256), *X509 Certificate Digest* (X5t#o), *X509 Certificates Digests* (SigX5ts) ou *X.509 Certificate Chain* (X5c). Além disso, a inclusão do parâmetro *Content Type* (Cty) pode ser necessária, dependendo do contexto da assinatura.

No JWS, o único parâmetro de cabeçalho definido como obrigatório é o *Algorithm* (Alg), que deve indicar o algoritmo criptográfico utilizado na assinatura. Esse parâmetro é protegido, garantindo que a assinatura só seja válida se um algoritmo reconhecido for especificado corretamente. Caso contrário, a assinatura será considerada inválida, pois não haverá um mecanismo confiável de verificação do conteúdo protegido por MAC [11]. Já no JAdES, o parâmetro obrigatório passa a ser o *Claiming Signing Time* (SigT), cuja função é registrar o momento exato em que o signatário realizou a assinatura digital. Para isso, o valor armazenado deve estar no formato Tempo Universal Coordenado (UTC), garantindo precisão e rastreabilidade.

O cabeçalho protegido *Critical* (Crit) tem a função de indicar quais parâmetros de extensão da assinatura devem ser interpretados e processados corretamente. Para isso, é gerada uma lista contendo esses elementos, a qual não pode estar vazia quando incluída. No contexto do JAdES, os parâmetros obrigatórios a serem processados incluem SigT, X5t#o e SigX5ts, conforme especificado pela normativa [10]. Já o parâmetro *Content Type* (Cty) é utilizado para definir o tipo de mídia contido no payload do JWS. Esse parâmetro se torna necessário quando há possibilidade de diferentes tipos de objetos estarem presentes no JWS payload, permitindo que a aplicação identifique corretamente a estrutura dos dados.

Os parâmetros *X5t#S256*, *X5t#o* e *SigX5ts* são classificados como protegidos e têm a função de armazenar o message digest, que contém o hash do documento assinado. O *X5t#S256*, introduzido originalmente no JWS, é opcional e está vinculado ao uso do algoritmo SHA-256. Já os parâmetros *X5t#o* e *SigX5ts*, definidos no JAdES, foram projetados para ampliar a flexibilidade do sistema de assinatura digital. O *X5t#o* permite o uso de algoritmos distintos do SHA-256, enquanto o *SigX5ts* é empregado quando múltiplos certificados digitais estão associados à mesma assinatura.

O parâmetro *X5c*, por sua vez, contém o certificado de chave pública X.509 ou a cadeia de certificados correspondente à chave utilizada para assinar digitalmente o JWS. Esse parâmetro armazena os certificados em formato Base64. Para que a assinatura seja validada corretamente, o X5c deve estar presente sempre que os parâmetros X5t#S256, X5t#o ou SigX5ts estiverem ausentes. Caso contrário, sua inclusão é opcional. Além disso, além dos parâmetros protegidos, o JAdES permite a inserção de parâmetros não protegidos, armazenados em uma estrutura chamada *etsi Unsigned (etsiU)*, cujo conteúdo também é codificado em Base64.

Com relação à necessidade de garantir documentos autocontidos no padrão HL7 FHIR, foi realizada uma adaptação para eliminar a

dependência de *hiperlinks* externos. Esse ajuste consiste em transferir todas as informações originalmente armazenadas em fontes externas para dentro do próprio documento JSON, substituindo as referências externas por identificadores internos. Como demonstrado na Figura 2, essa abordagem assegura que todos os dados essenciais permaneçam incorporados no arquivo. Dessa forma, a prescrição digital se mantém autossuficiente e imutável, permitindo sua validação independente. Esse ajuste se torna fundamental, pois ao garantir a persistêncioa dos dados diretamente no documento assinado, eliminam-se riscos associados à volatilidade das informações obtidas de maneira dinâmica na web.

```
{
    "location": {
        "reference": "urn:uuid:72f58493-6a0c-4165-9868-
    e21616e06497"
    },

    //other informations...

    "fullUrl": "urn:uuid:72f58493-6a0c-4165-9868-
    e21616e06497",
    "resource": {
        "resourceType": "Location",
        "meta": {
            "profile": [
                "http://www.saude.gov.br/fhir/r4/
    StructureDefinition/BRFarmacia"
            ]
        },
        "mode": "instance",
        "status": "active",
        "name": "Farmacia de teste",
        "address": {
            "text": "Rua das Flores, 123, Centro, Florian
    \u00f3polis, SC"
        }
    }
}
```

Figure 2: Exemplo de referência local sem url externo

Antes que a assinatura digital seja aplicada ao documento FHIR, é essencial validar os dados do profissional responsável pelo processo, seja ele médico ou farmacêutico. Para isso, foi necessário o desenvolvimento de uma API de validação, denominada validador, capaz de verificar as informações do profissional, incluindo CRM, estado de atuação, Cadastro de Pessoa Física (CPF) e nome completo. Essa API tem a função de garantir que apenas profissionais devidamente registrados possam assinar ou dispensar receitas digitais. No momento da assinatura, o validador também realiza a conferência entre os dados do profissional e o certificado digital utilizado na assinatura, assegurando que ambos estejam corretamente vinculados.

Além da validação profissional, é necessário garantir que a assinatura digital utilizada esteja conforme os padrões brasileiros de certificação digital (PBAD). Para isso, foi desenvolvida uma terceira API, denominada verificador de conformidade, responsável por analisar os parâmetros da assinatura e verificar se ela está vinculada a uma âncora de confiança reconhecida no Brasil. Além disso, essa API confirma a validade do certificado do signatário e de toda a cadeia de certificação, assegurando que nenhum dos certificados envolvidos no processo tenha sido revogado.

Como tanto o assinador quanto o verificador de conformidade realizam operações relacionadas ao certificado digital do usuário, algumas de suas funcionalidades foram unificadas em uma biblioteca central, chamada core. Após a verificação da conformidade da assinatura, o documento assinado contendo as informações do médico, paciente e medicamentos prescritos é registrado na *Blockchain*. Durante esse processo, é gerado um identificador único aleatório para cada prescrição, que é capaz de resgatar os seguintes dados: um identificador único, a data de registro da prescrição, a lista de medicamentos receitados e suas respectivas quantidades.

A recuperação das informações necessárias para a dispensação dos medicamentos é feita por meio da chave da prescrição. Durante esse processo, o sistema realiza a validação da prescrição por meio do validador e do verificador de conformidade, garantindo que a receita seja autêntica e que existam medicamentos disponíveis para dispensação. O farmacêutico responsável pode então optar por dispensar todos os medicamentos prescritos ou apenas uma parte deles, dependendo da necessidade do paciente.

Durante a dispensação, o farmacêutico deve fornecer informações essenciais sobre o estabelecimento, incluindo nome, Cadastro Nacional de Pessoa Jurídica (CNPJ) e contato, garantindo que o processo esteja devidamente documentado. Assim como ocorre na verificação dos médicos, os dados do farmacêutico são validados em bases de dados do Conselho Federal de Farmácia (CFF). Se as informações forem consistentes, o farmacêutico terá acesso à lista de medicamentos disponíveis para dispensação e poderá registrar a entrega dos fármacos. Ao final desse processo, um documento em formato FHIR é gerado contendo os detalhes da dispensação. Esse documento deve então ser assinado digitalmente e submetido ao mesmo processo de verificação da prescrição, antes de ser armazenado na *Blockchain*.

Na *Blockchain Hyperledger Fabric*, cada plataforma de prescrição atua como um nó da rede, permitindo que diferentes instâncias do sistema realizem registros de prescrição e dispensação. Cada nó pode inserir informações de forma independente, mas apenas um nó central tem acesso a todas as transações registradas na rede. Dessa forma, o modelo adotado é o de uma *Blockchain* permissionada, exigindo um mínimo de três nós ativos para garantir a confiabilidade do sistema. Em uma implementação oficial do projeto para abrangência nacional, o nó central seria idealmente operado por um órgão governamental responsável pelo gerenciamento dos registros de prescrição digital. Para proteger os dados pessoais de pacientes, médicos e farmacêuticos, o sistema garante que, durante a busca por uma prescrição, apenas as informações essenciais para a dispensação sejam disponibilizadas ao farmacêutico. Dessa maneira, o profissional não tem acesso aos dados pessoais do paciente, garantindo conformidade com a Lei Geral de Proteção de Dados (LGPD).

Após a implementação de todo o fluxo do sistema, restava definir um meio eficiente para que o paciente tivesse acesso à sua prescrição digital. A solução adotada foi a geração de um documento em formato PDF, contendo um QR Code que armazena a chave da prescrição. Essa chave permite que o paciente consulte informações sobre os medicamentos prescritos e os estabelecimentos onde pode realizar a dispensação. Na prática, isso significa que, ao assinar

uma prescrição digital, o médico está gerando dois arquivos. Um arquivo JSON, que é a prescrição oficial registrada na Blockchain e um arquivo PDF, que serve como representação visual da prescrição, facilitando o acesso e compreensão pelo paciente.

Portanto para a execução do projeto foram necessárias as APIs de validação, verificação de conformidade, realização de assinatura, biblioteca *core* comum, comunicação com bases de dados da CFM e CFF, umas *Blockchain* em *Hyperledger Fabric* e uma pequena aplicação de interface para viabilizar a visualização do funcionamento de todo o sistema em conjunto com a criação do PDF do paciente, o que culminou na arquitetura mostrada pela Figura 3.

Assim a definição de tecnologia com garantia de integridade do processo, validação de crendenciais dos profissionais da saúde, verificação de conformidade das assinaturas e gerenciamento de dispensações de medicamentos foi construído com três pilares de componentes tecnológicos:

- Padrão HL7 FHIR de interoperabilidade: Arquivo JSON no padrão adaptado para garantir a geração de documentos autocontidos sem referências externas.
- Assinatura digital JAdES: Implementação de uma API para assinatura digital qualificada com implementação robusta de parâmetros de forma a garantir a segurança do documento gerado.
- *Blockchain*: Uso de Hyperledger Fabric para registrar prescrições e dispensações de forma imutável, garantindo assim a rastreabilidade dos documentos gerados.

4.3 Avaliação do sistema

Para assegurar o funcionamento adequado das APIs, foram implementados testes unitários para validar suas funcionalidades. A API de assinatura digital passou por verificações para garantir que todos os parâmetros obrigatórios estivessem corretamente inseridos na assinatura, que o processo de assinatura fosse executado corretamente e que diferentes artefatos de teste confirmassem a inclusão do parâmetro *digest algorithm*. Já a API de verificação de conformidade foi submetida a testes que avaliaram a validação de assinaturas corretas e incorretas, a proteção contra repúdio da assinatura, a checagem da cadeia de certificação e a conferência da validade dos parâmetros utilizados na assinatura digital.

Os testes aplicados à API de validação de credenciais tiveram como objetivo garantir a correção das informações do profissional de saúde, verificando se os dados fornecidos estavam coerentes com os registros das bases do CFM e do CFF. Além disso, foi validado se as credenciais estavam sendo devidamente registradas tanto na prescrição quanto na dispensação de medicamentos. Também foram conduzidos testes específicos para verificar a integridade dos registros no banco de dados, garantindo que a prescrição e a dispensação fossem devidamente processadas e armazenadas de maneira consistente.

Os testes realizados na *Blockchain* abrangeram tanto prescrições e dispensações válidas, garantindo que fossem corretamente registradas e acessadas, quanto tentativas inválidas, verificando a rejeição de registros incorretos ou fraudulentos. Além disso, foram conduzidos testes para validar a consulta de prescrições, focando na capacidade da *Blockchain* de retornar corretamente a quantidade de medicamentos restantes para cada prescrição. Esse teste garantiu que, após cada dispensação, o sistema atualizasse de forma precisa o número de medicamentos disponíveis, prevenindo inconsistências e possíveis erros na distribuição.

Durante o desenvolvimento deste trabalho, foram realizadas iterações e refinamentos para aprimorar a clareza textual por meio do uso de inteligência artificial generativa ao longo de todo o texto do artigo. Essa tecnologia foi empregada para otimizar e simplificar o texto na seção "abstract", auxiliar na organização e estruturação da seção de discussão e resultados, e aprimorar a coesão dos parágrafos na conclusão, garantindo uma melhor apresentação das ideias.

5 Resultados e Discussão

5.1 Conceitos desenvolvidos

A pesquisa demonstrou uma viabilidade técnica para integração do padrão HL7 FHIR com assinatura digitais JAdES para padronizar as informações de diferentes centros e garantir a interoperabilidade das informações, assim como alcançou a criação de arquivo em padrão FHIR em documento com informações autocontidas através da exclusão de *hiperlinks*. Além de definir um sistema robusto contra prevenção de falsificações através das validações nas bases de dados CFM e CFF.

Também determinou a criação de uma nova classe de dispensação de medicamentos, a dispensação parcial, que por sua vez concede uma maior flexibilidade para os pacientes e tem a capacidade de auxiliar no gerenciamento do estoque de medicamentos. Por ser um conceito totalmente novo possui um peso significativo como resultado do projeto no qual ampliou o processo de dispensação de medicamentos e também trouxe uma nova visão de melhorias necessárias para viabilizar sua aplicação.

Nesse estudo também foi explorado a capacidade de uso das propriedades da *Blockchain* como uma solução robusta com o propósito resolver os desafios relacionados ao controle de medicamentos de uso especial, para assim aumentar a segurança e mitigar as chances de desvio ou abuso do uso desses medicamentos de forma rigorosa de acordo com a regulamentação brasileira com um sistema mais confiável e transparente.

5.2 Contribuições do estudo

A principal contribuíção científica desta pesquisa é a criação de um sistema digital inovador para prescrição e dispensação de medicamentos que integra três tecnologias de forma inédita: *Blockchain*, assinaturas digitais JAdES e o padrão de interoperabilidade HL7 FHIR. Essa abordagem permite que documentos médicos sejam gerados de forma segura, interoperável e imutável, eliminando a necessidade de referências externas voláteis e garantindo a autenticidade das informações. Além disso, a solução facilita a rastreabilidade de medicamentos controlados, reduzindo risco de falsificação e melhorando a segurança regulatória.

Diferentemente de estudos atneriores que focam nas tecnologias de forma isolada, este trabalho integra as tecnologias em um fluxo completo e validado, cobrindo desde a prescrição até a dispensação dos medicamnetos. A proposta não se limita a um modelo teórico, assim ela foi validada com uma prova de conceito (PoC) implementada em ambiente controlado, demonstrando sua viabilidade para aplicação real no setor de saúde.

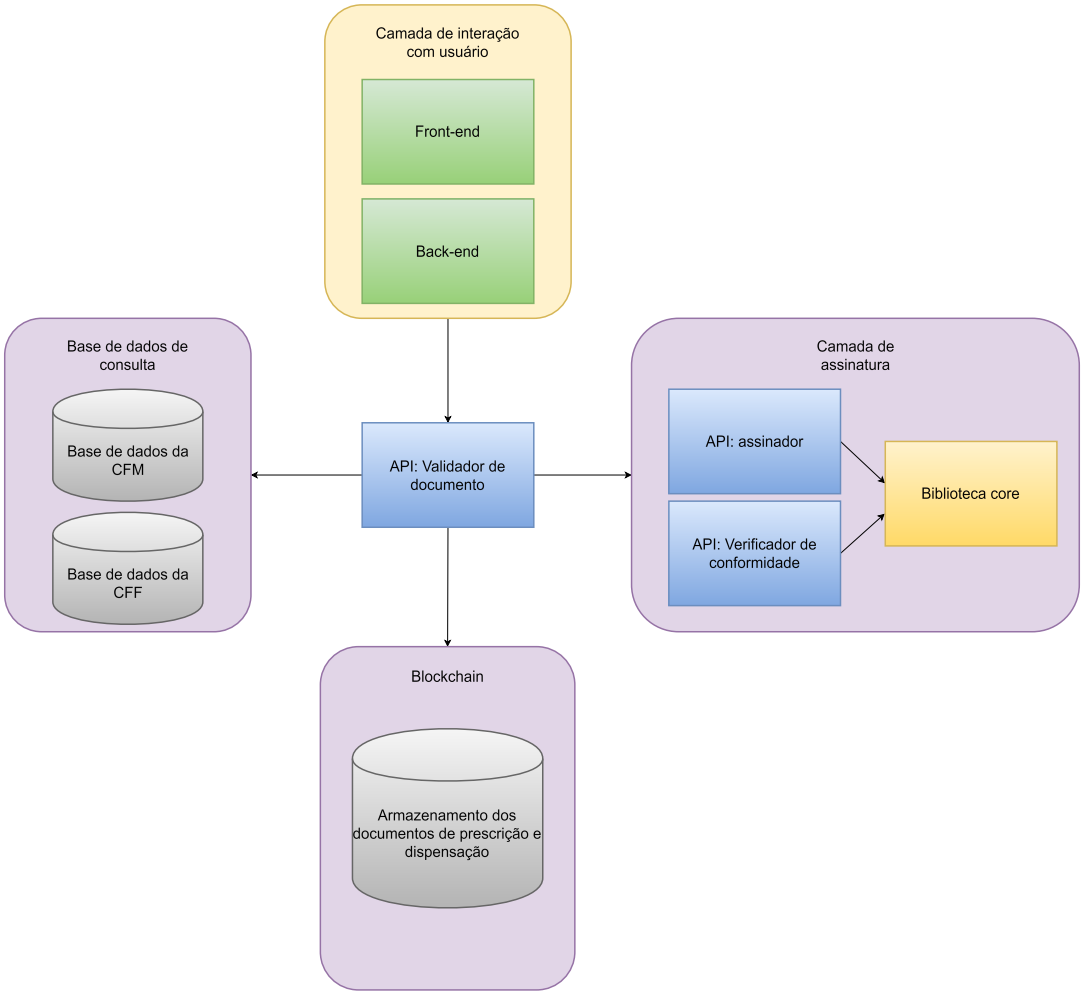

Figure 3: Diagrama de arquitetura do projeto. Atualizada de [21]

Essa inovação transforma o processo tradicional de prescrição e dispensação, permitindo que s documentos sejam gerados de forma totalmente digital, com assinatura eletrônica qualificada e armazenamento seguro com o uso da *Blockchain* permissionada. De forma adicional, introdução do conceito de dispensação parcial representa um avanço, conferindo mais flexibilidade ao paciente e otimizando a gestão de remédios a serem dispensados na receita sem comprometer a conformidade regulatória.

5.3 Limitações encontradas

Embora o sistema proposto tenha sido validado em um ambiente controlado, sua aplicação em cenários reais exige considerações adicionais relacionadas à adaptação de sistemas legados, aceitação dos profissionais de saúde e conformidade regulatória.

A integração com sistemas legados é um dos principais desafios, visto que hospitais, clínicas e farmácias utilizam plataformas heterogêneas, muitas delas sem suporte nativo ao padrão HL7 FHIR. Para mitigar essa barreira, a abordagem foi projetada para permitir a interoperabilidade progressiva, possibilitando que sistemas existentes continuem operando enquanto adotam gradualmente os novos padrões. Um exemplo dessa estratégia poode ser visto na RNDS, que já promove a adoção gradual do HL7 FHIR em diferentes instituições, reduzindo impactos operacionais.

A aceitação dos profissionais da saúde também é um fator crítico. A adoção de novas tecnologias no setor costuma encontrar resistência devido à necessidade de treinamento e adaptação a novos fluxos de trabalho. No entanto, iniciativas recentes de digitalização, como a implementação da prescrição digital na rede pública durante a pandemia da COVID-19, demonstraram que a transição para modelos digitais é viável quando os benefícios são claros, especialmente em termos de segurança, rastreabilidade e redução de burocracia. Para garantir a adesão, o modelo proposto mantém interfaces familiares aos profissionais, minimizando a curva de aprendizado.

Do ponto de vista regulatório, a adoção de *Blockchain* para rastreamento de medicamentos exige conformidade com diretrizes da Agência Nacional de Vigilância Sanitária (ANVISA) e a Lei Geral de Proteção de Dados (LGPD). O sistema proposto atende a esses

requisitos ao utilizar uma *Blockchain* permissionada, onde apenas entidades certificadas podem operar nós da rede, garantindo privacidade e controle sobre os dados sensíveis. Essa abordagem já é explorada em países como Estônia e Canadá, onde *Blockchain* tem sido usada para gerenciar registros médicos com altos padrões de segurança e governança. Esses fatores impactam na viabilidade de implementação de um teste em ambiente real.

6 Conclusão

Em resumo a pesquisa apresenta uma inovação no processo de prescrição e dispensação de medicamentos, através da digitalização e adoção do padrão HL7 FHIR em conjunto com o uso de assinatura JAdES e pela interoperabilidade das informações através de uma *Blockchain* permissionada. Os resultados demonstraram uma viabilidade técnica e a segurança do sistema. Destacam-se a criação de documentos autocontidos em padrão FHIR, o conceito de dispensação parcial e a solução de *Blockchain* garantia de rastreabilidade.

Para trabalhos futuros, melhorias voltadas à experiência do paciente podem ser exploradas e aplicação em um contexto controlado com poucos estabelecimentos pode ser realizado. A inclusão de funcionalidades como notificações automáticas sobre a validade da receita, lembretes de retirada de medicamentos e acesso a históricos detalhados de prescrições e dispensações pode tornar o sistema mais acessível e funcional. Além disso, a criação de interfaces intuitivas, como aplicativos móveis, permitiria que os pacientes gerenciassem suas receitas de forma mais prática e autônoma, promovendo maior engajamento e adesão ao tratamento.

Acerca de aplicação do sistema com estabelecimentos em contexto real para avaliar a eficiência, segurança e o impacto prático. Esse tipo de estudo permitiria validar o sistema em cenários reais de uso e identificar ajustes para adoção em larga escala. A digitalização do processo de prescrição e dispensação, associada a essas inovações, tem o potencial de melhorar significativamente a experiência dos pacientes, tornando o sistema de saúde mais eficiente, seguro e orientado às necessidades individuais.

References

[1] [n. d.]. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. http://data.europa.eu/eli/reg/2014/910/oj/eng Legislative Body: EP, CONSIL.

[2] Duane Bender and Kamran Sartipi. 2013. HL7 FHIR: An Agile and RESTful approach to healthcare information exchange. In *Proceedings of the 26th IEEE International Symposium on Computer-Based Medical Systems* (Porto, Portugal, 2013-06). IEEE, 326–331. https://doi.org/10.1109/CBMS.2013.6627810

[3] Shekha Chenthara. 2021. PRIVACY PRESERVATION OF ELECTRONIC HEALTH RECORDS USING BLOCKCHAIN TECHNOLOGY: HEALTHCHAIN. (2021).

[4] Conselho Federal de Medicina. 2021. Resolução CFM nº 2.299/2021. https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2021/2299. Acessado em: 09 jun. 2024.

[5] Maja Georgioska. 2020. Application of Digital Signatures in the Electronic System for Public Procurement in Republic of North Macedonia. (2020).

[6] Julian Gruendner, Christian Gulden, Marvin Kampf, Sebastian Mate, Hans-Ulrich Prokosch, and Jakob Zierk. 2021. A Framework for Criteria-Based Selection and Processing of Fast Healthcare Interoperability Resources (FHIR) Data for Statistical Analysis: Design and Implementation Study. 9, 4 (2021), e25645. https://doi.org/10.2196/25645

[7] Health Level Seven International. 2023. FHIR Modules. https://hl7.org/fhir/modules.html. Acessado em: 09 jun. 2024.

[8] Juan-Carlos Cruellas Ibarz. 2020. Bringing JSON signatures to ETSI AdES framework: Meet JAdES signatures. 71 (2020), 103434. https://doi.org/10.1016/j.csi.2020.103434

[9] Name Ibarz. 2021. Development of a tool for validating ETSI AdES digital signatures as defined by the European Standard ETSI EN 319 102-1. (2021).

[10] European Telecommunications Standards Institute. 2021. *Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures.* https://www.etsi.org/deliver/etsi_ts/119100_119199/11918201/01.01.01_60/ts_11918201v010101p.pdf

[11] Michael B. Jones, John Bradley, and Nat Sakimura. 2015. JSON Web Signature (JWS). https://doi.org/10.17487/RFC7515 Num Pages: 59.

[12] Mirosław Kutyłowski and Przemysław Błaśkiewicz. 2023. Advanced Electronic Signatures and eIDAS – Analysis of the Concept. 83 (2023), 103644. https://doi.org/10.1016/j.csi.2022.103644

[13] Ministério da Saúde do Brasil. 2020. Rede Nacional de Dados em Saúde (RNDS). https://www.gov.br/saude/pt-br/composicao/seidigi/rnds/rnds. Acessado em: 09 jun. 2024.

[14] Karen A Monsen, Laura Heermann, and Karen Dunn-Lopez. 2023. FHIR-up! Advancing knowledge from clinical data through application of standardized nursing terminologies within HL7® FHIR®. 30, 11 (2023), 1858–1864. https://doi.org/10.1093/jamia/ocad131

[15] Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. 2017. Blockchain. 59, 3 (2017), 183–187. https://doi.org/10.1007/s12599-017-0467-3

[16] Nurzhan Nurseitov, Michael Paulson, Randall Reynolds, and Clemente Izurieta. 2009. Comparison of JSON and XML Data Interchange Formats: A Case Study. (2009).

[17] Presidência da República do Brasil. 1957. Lei nº 3.268, de 30 de setembro de 1957. http://www.planalto.gov.br/ccivil_03/leis/l3268.htm. Acessado em: 09 jun. 2024.

[18] Presidência da República do Brasil. 1960. Lei nº 3.820, de 11 de novembro de 1960. http://www.planalto.gov.br/ccivil_03/leis/l3820.htm. Acessado em: 09 jun. 2024.

[19] Presidência da República do Brasil. 2020. Lei nº 14.063, de 23 de setembro de 2020. https://www.in.gov.br/en/web/dou/-/lei-n-14.063-de-23-de-setembro-de-2020-278574432. Acessado em: 09 jun. 2024.

[20] Alex Roehrs, Cristiano A Da Costa, Rodrigo R Righi, André H Mayer, Valter F Da Silva, José R Goldim, and Douglas C Schmidt. 2021. Integrating multiple blockchains to support distributed personal health records. 27, 2 (2021), 146045822110075. https://doi.org/10.1177/14604582211007546

[21] Liverson Severo and Jean Martina. 2025. Digital Medication Prescription System with JSON. In *Proceedings of the 18th International Joint Conference on Biomedical Engineering Systems and Technologies - Volume 2: HEALTHINF*. INSTICC, SciTePress, 834–843. https://doi.org/10.5220/0013315700003911

[22] Carina Nina Vorisek, Moritz Lehne, Sophie Anne Ines Klopfenstein, Paula Josephine Mayer, Alexander Bartschke, Thomas Haese, and Sylvia Thun. 2022. Fast Healthcare Interoperability Resources (FHIR) for Interoperability in Health Research: Systematic Review. 10, 7 (2022), e35724. https://doi.org/10.2196/35724