Journal of Health Informatics

J Health Inform. 2026;18:e1814
DOI: https://doi.org/10.59681/2175-4411.v18.iEspecial.2026.1814

ARTIGO COMPLETO
CBIS 2026

Uma política de assinatura digital para a interoperabilidade baseada em FHIR

A digital signature policy for FHIR-based interoperability

Daniel Nogueira da Costa[1], Murilo Lopes da Luz[1], Mariana Soller Ramada[1], Leonardo Cortes-Filho[1], Caio Castro Miranda[1], Carlos Augusto Gonçalves Tibiriçá[2], Diana Ferreira Guimarães[2], Luiselena Luna Esmeraldo[2], Renata Dutra Braga[1], Juliana Pereira de Souza-Zinader[1] ✉

ORCID: 0009-0003-0957-959X · 0009-0008-2645-1383 · 0000-0003-2198-9754 · 0009-0000-0425-628X · 0009-0004-0827-5049 · 0000-0002-1455-0906 · 0009-0003-2318-3110 · 0000-0002-7135-5947 · 0000-0002-3448-0343 · 0009-0005-7780-4626

[1] Instituto de Informática, Universidade Federal de Goiás, Goiânia (GO), Brasil.

[2] Superintendência de Tecnologia, Inovação e Saúde Digital, Secretaria de Saúde do Estado de Goiás, Goiânia (GO), Brasil.

FICHA DO ARTIGO

TIPO
Artigo completo · CBIS 2026

IDENTIFICADOR
e1814

DOI
10.59681/2175-4411.v18.iEspecial.2026.1814

RECEBIDO
17/05/2026

APROVADO
20/07/2026

PROCESSO DE AVALIAÇÃO
Double Blind Review

EDITOR RESPONSÁVEL
Juliano de Souza Gaspar

ACESSO
Aberto, CC BY 4.0

AUTOR CORRESPONDENTE
Juliana Pereira de Souza-Zinader
juliana_souza@ufg.br

LICENÇA

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

CC BY 4.0

RESUMO

Objetivo: Propor uma política de assinatura digital para informação em saúde registrada em instâncias de recursos FHIR (Fast Healthcare Interoperability Resources), estabelecendo princípios técnicos, semânticos e operacionais do processo de assinatura. A assinatura digital é um mecanismo criptográfico para a garantia da autenticidade, integridade e não repúdio da informação em saúde. **Método:** O método DSR (Design Science Research) é empregado para o desenvolvimento de artefatos relevantes à resolução de problemas do mundo real. **Resultados:** A proposta atende às orientações oficiais HL7 para assinaturas digitais, sendo aderente a diretrizes abstraídas de publicações científicas recentes. Foi desenvolvido um processo de assinatura em 14 etapas, em nível de especificação adequado à implementação da proposta, distintamente de iniciativas anteriores. **Conclusão:** A política promove assinaturas reproduzíveis, verificáveis em um contexto amplo de troca de dados regional usando FHIR. Um processo de validação da política está em curso, englobando aspectos como conformidade e segurança jurídica.

Descritores: segurança computacional; interoperabilidade da informação em saúde; registros eletrônicos de saúde.

ABSTRACT

Objective: To propose a digital signature policy for health information recorded in instances of FHIR (Fast Healthcare Interoperability Resources) resources, establishing technical, semantic, and operational principles of the signature process. Digital signatures are a cryptographic mechanism for guaranteeing the authenticity, integrity, and non-repudiation of health information. **Method:** The DSR (Design Science Research) method is employed to develop artifacts relevant to solving real-world problems. **Results:** The proposal meets the official HL7 guidelines for digital signatures, adhering to guidelines abstracted from recent scientific publications. A 14-step signature process was developed, at a specification level suitable for the implementation of the proposal, distinct from previous initiatives. **Conclusion:** The policy promotes reproducible, verifiable signatures in a broad context of regional data exchange using FHIR. A policy validation process is underway, encompassing aspects such as compliance and legal security.

Keywords: computer security; health information interoperability; electronic health records.

CBIS 2026 XXI CONGRESSO BRASILEIRO DE INFORMÁTICA EM SAÚDE

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

COMO CITAR ESTE ARTIGO: da Costa DN, da Luz ML, Ramada MS, Cortes-Filho L, Miranda CC, Tibiriçá CAG, et al. Uma política de assinatura digital para a interoperabilidade baseada em FHIR. J Health Inform 2026;18:e1814. doi: https://doi.org/10.59681/2175-4411.v18.iEspecial.2026.1814

1 INTRODUÇÃO

FHIR (*Fast Healthcare Interoperability Resources*) é um padrão para a interoperabilidade de informação em saúde, que é adotado em diversos países, inclusive no Brasil. A adoção do FHIR tem promovido a integração da informação em saúde entre sistemas de saúde, mas também expôs novos vetores de risco associados à autenticidade, integridade, não repúdio e rastreabilidade das informações. À medida que laudos, prescrições e sumários de alta, dentre outros, são compartilhados, torna-se imprescindível tratar os vetores de risco.

A assinatura digital, nesse contexto, surge como o mecanismo criptográfico para assegurar que um registro clínico mantenha um vínculo indissociável com a identidade de seu emissor, garantindo a validade jurídica necessária para a confiança na informação, além de contemplar processos de auditoria e conformidade [1].

Assinaturas digitais são sequências de bytes. No processo de geração de uma assinatura digital, o conteúdo a ser assinado (e.g., um laudo) é preparado resultando em uma sequência de bytes intermediária, a partir da qual a assinatura será criada. A assinatura digital ocorre pela geração de uma segunda sequência de bytes, obtida a partir da primeira sequência, onde a segunda também inclui informações do signatário (e.g., o certificado digital) [1].

No processo de validação da assinatura, é possível averiguar: se o conteúdo considerado na validação corresponde ao conteúdo assinado (prova criptográfica de que o conteúdo não foi alterado); e qual certificado digital foi utilizado no processo de assinatura (prova de que a assinatura digital foi feita a partir de um dado certificado digital). Com respeito ao signatário, a chave privada correspondente ao seu certificado digital é usada no processo de geração da assinatura, e a chave pública do certificado é usada no processo de validação da assinatura [1].

Segundo a organização mantenedora de especificações FHIR (HL7®), o padrão FHIR não objetiva definir uma política de assinatura digital, que estrutura e normatize a geração e validação de assinaturas, mas possui diretrizes gerais sobre os recursos FHIR vocacionados à implementação de assinaturas [2,3]. Noutras palavras, cabe ao contexto em questão, possivelmente nacional, a definição e implementação de uma política de assinatura digital baseada em FHIR.

O objetivo deste trabalho é propor uma política de assinatura digital para o ecossistema FHIR, estabelecendo princípios técnicos, semânticos e operacionais do processo de assinatura de documentos clínicos. A política orienta a forma como recursos FHIR são preparados, padronizados de forma canônica (canonicalizados), assinados e validados. A política é particularmente relevante para garantir consistência, independentemente da implementação, linguagem de implementação ou infraestrutura.

Em termos acadêmicos, não são muitas as comunicações científicas que lidam com a proposição de uma política de assinatura digital. Na perspectiva de publicações *online*, destacam-se o direcionamento oficial da HL7® *International*, que em essência não define uma política de assinatura [2], bem como a proposta do projeto Da Vinci [4], que reúne casos de uso em cenários de troca de informação sobretudo no sistema de saúde dos Estados Unidos. Por outro lado, o presente estudo especifica uma política detalhada e operacional de assinatura digital para ecossistemas FHIR, permitindo a geração e a validação por múltiplos atores [5].

Esta pesquisa resulta de uma colaboração entre a Secretaria de Saúde do Estado de Goiás (SES-GO) e a Universidade Federal de Goiás (UFG), Brasil, com foco na interoperabilidade em saúde e na educação continuada. A Seção 2 apresenta o método aplicado no desenvolvimento da pesquisa. As orientações compiladas a partir de documentos HL7 *International*, bem como diretrizes a políticas de assinatura digital no contexto FHIR, são exploradas na Seção 3. A Seção 4 discute o processo de geração de assinatura digital que caracteriza a presente proposta. As conclusões e perspectivas futuras são postas na Seção 5.

2 MÉTODOS

O trabalho emprega o método descrito em [6], denominado *Design Science Research* (DSR), envolvendo o desenvolvimento de artefatos relevantes para a resolução de problemas do mundo real. O método DSR abstrai o conhecimento na forma de princípios de *design*, modelos e impactos do uso de tecnologias [7].

A pesquisa foi conduzida por 12 pesquisadores (os dez autores e dois professores doutores da Universidade Federal de Goiás que colaboraram com a investigação), a partir de dezembro de 2024, encontrando-se em andamento. A definição da política originou o guia de implementação público que a documenta [5], cuja primeira versão foi concluída em meados de 2025; as implementações de referência foram concluídas ao final de 2025. As atividades combinaram reuniões quinzenais de acompanhamento com a área de negócio demandante, nas quais a assinatura digital constituía um dos tópicos, e sessões técnicas de dedicação variável, conforme a demanda de cada iteração do método. Como apoio às atividades, foram utilizados: a linguagem FHIR Shorthand (FSH), para a definição precisa dos artefatos FHIR da política; o IG Publisher, para a geração do guia de implementação; o validador oficial FHIR, para a verificação de conformidade das instâncias; e uma implementação de referência desenvolvida em Java (Maven/Spring), construída sem dependências de bibliotecas FHIR de terceiros (de

modo que a implementação derivasse exclusivamente da especificação da política) e testada com certificado ICP-Brasil real.

As atividades previstas no método e instanciadas à presente pesquisa são sucintamente descritas a seguir.

Conscientização do problema. O problema emergiu de demanda concreta da área de negócio da SES-GO: soluções de informação em saúde que requeriam assinatura digital de conteúdos JSON com validade em território nacional. A investigação preliminar não identificou normatização ou documentação suficiente para assinaturas digitais sobre conteúdo JSON no contexto nacional, inclusive junto ao Instituto Nacional de Tecnologia da Informação (ITI). Os pesquisadores envolvidos na investigação estudam os trabalhos relacionados e, por meio de reuniões coletivas e individuais, elaboram uma compreensão do problema e sua solução, para definir: classificação do problema, impacto do problema, objetivos/metas e especificidade da solução.

Sugestão. Os pesquisadores definem diretrizes fundamentais à solução do problema, conforme a literatura, a saber: canonicalização e serialização; validação de longo prazo; granularidade e escopo da assinatura; e vinculação semântica. São também identificadas as orientações oficiais sobre assinaturas digitais, segundo HL7®. Ao final dessa atividade, é produzida uma proposta preliminar da política de assinatura, a qual deverá evoluir ao longo da aplicação do método.

Desenvolvimento e Avaliação. As atividades de desenvolvimento e avaliação representam uma abordagem iterativa e incremental. Em cada iteração, os pesquisadores realizam as seguintes tarefas:

- Definição de objetivos: As necessidades de negócio e os requisitos de software são refinados, pois ambos são aspectos orientadores da iteração.
- Execução incremental: A versão corrente da política é modificada de acordo com os objetivos; as alterações são registradas.
- Validação incremental: A política modificada é avaliada com base em estratégias de consenso, nas reuniões quinzenais com a área de negócio: problemas, resultados do desenvolvimento e conflitos de especificação eram discutidos até a convergência sobre os direcionamentos, e os encaminhamentos acordados orientavam a iteração seguinte.

Conclusão. Os resultados obtidos são consolidados, as contribuições científicas são comunicadas, de modo que o conhecimento gerado durante a pesquisa seja adequadamente disseminado [7].

3 RESULTADOS

Esta seção consolida dois dos artefatos gerados na atividade *Sugestão* do método DSR (Seção 2): as orientações oficiais sobre assinaturas digitais, segundo HL7® *International*, e diretrizes fundamentais à proposição de políticas de assinatura no ecossistema FHIR.

3.1 Orientação segundo HL7® sobre assinaturas digitais

A orientação oficial da HL7® *International* sobre o objeto em estudo destaca que o FHIR não define uma política de assinatura. Contudo, o FHIR fornece o tipo de dados para registro da assinatura digital, uma estrutura canônica por meio do tipo de dados *Signature*, que é encontrado no elemento *signature* de vários recursos FHIR, tal como o recurso *Provenance* [2,3].

A Figura 1 introduz a estrutura do tipo de dados *Signature*. Uma instância de *Signature* contém uma representação de uma assinatura e seu contexto de suporte em um formato acessível pelo FHIR. Alguns dos elementos em *Signature* são realçados a seguir: *targetFormat*: representa o formato técnico dos recursos assinados; *sigFormat*: representa o formato técnico da assinatura; *who*: identifica o agente responsável pela assinatura, que pode ser uma pessoa, um dispositivo, uma organização, um serviço externo, etc; *data*: constitui a sequência de bytes em si da assinatura, e representa a evidência matemática de integridade, autenticidade e não repúdio do conteúdo assinado.

Em [2] há ainda orientações sobre casos de uso, validação e interoperabilidade: assinatura de documentos clínicos estruturados, assinaturas encadeadas (por exemplo, múltiplos atores adicionando assinaturas incrementais), assinaturas de transações e uso em trilhas de auditoria. O texto conclui reforçando que o ecossistema FHIR deve adotar práticas criptográficas robustas, métodos de serialização determinísticos e políticas de gestão de chaves maduras para garantir segurança e confiabilidade na troca de informações clínicas.

3.2 Diretrizes a políticas de assinatura digital no contexto FHIR

Conforme ressaltado na Subseção 3.1, a especificação FHIR deixa a assinatura digital como uma solução específica da implementação, sem a definição de padronização de algoritmos ou protocolos. Uma política propositiva aborda requisitos funcionais, criptográficos, operacionais e regulatórios para garantir integridade, autenticidade, não repúdio e validade. Ou seja, é necessária a preservação da semântica da informação ao longo do tempo.

Figura 1. Estrutura do tipo de dados Signature da versão 4 do HL7 FHIR.

Name	Flags	Card.	Type	Description & Constraints
Signature	TU		Element	A Signature - XML DigSig, JWS, Graphical image of signature, etc. Elements defined in Ancestors: id, extension
type	Σ	1..*	Coding	Indication of the reason the entity signed the object(s) Signature Type Codes (Preferred)
when	Σ	1..1	instant	When the signature was created
who	Σ	1..1	Reference(Practitioner | PractitionerRole | RelatedPerson | Patient | Device | Organization)	Who signed
onBehalfOf	Σ	0..1	Reference(Practitioner | PractitionerRole | RelatedPerson | Patient | Device | Organization)	The party represented
targetFormat		0..1	code	The technical format of the signed resources MimeType (Required)
sigFormat		0..1	code	The technical format of the signature MimeType (Required)
data		0..1	base64Binary	The actual signature content (XML DigSig. JWS, picture, etc.)

Fonte: HL7 FHIR [8].

A formulação de uma política de assinatura digital em FHIR exige atenção à (ao):

- *Integridade*: Garantia de que o conteúdo assinado foi preservado e não foi adulterado ou sofreu modificação maliciosa.
- *Autenticidade*: Identificação inequívoca da entidade (humana ou sistema) originadora da assinatura.
- *Não repúdio*: Impossibilidade de negar a autoria. Havendo um carimbo de tempo associado, garante-se que a assinatura foi gerada em um dado instante no tempo.
- *Determinismo de verificação*: O processo de verificação da assinatura deve produzir resultados consistentes e reproduzíveis, independentemente das ferramentas utilizadas, desde que em conformidade com a política.
- *Interoperabilidade*: Uso de padrões abertos (e.g., JSON Web Signature (JWS)/RFC 7515) em detrimento de soluções proprietárias, visando maximizar a compatibilidade entre diferentes atores, plataformas e implementações.

A seguir estão alguns dos elementos fundamentais para a proposição de uma política de assinatura digital em FHIR, inspirados em [1,9,10].

Canonicalização e serialização. Para viabilizar uma assinatura digital, os conteúdos de saúde precisam ser serializados e canonicalizados. A serialização orienta como os dados são representados na forma de "sequência de bytes". Por sua vez, a canonicalização é o processo de padronizar a representação de um dado em uma forma única e determinística. Ambos os processos são aplicados a dados de diversas naturezas, tais como texto, código, número, imagem e/ou vídeo. Uma política de assinatura requer uma preparação preliminar pela exclusão de elementos não ligados ao conteúdo a ser assinado, tais como identificadores internos, bem como a escolha de um algoritmo de canonicalização, visando uma representação uniforme ao conteúdo clínico. Se a política prevê a representação da informação em formato JSON, é pertinente considerar o uso de normas como a RFC 8785 (*JSON Canonicalization Scheme*).

Padrão de assinatura digital. É pertinente a adoção de padrões AdES (*Advanced Electronic Signatures*), que estruturam a assinatura digital pela inclusão de metadados de assinatura, tais como certificados, políticas de validação e listas de revogação. Como exemplos, há o XAdES (para XML) e o JAdES (para JSON), neste último o JAdES-B (*Baseline*) representa o nível mais básico de assinatura no padrão JAdES.

Granularidade e escopo da assinatura. O conteúdo a ser assinado pode ser composto por vários itens de informação, formando uma rede de recursos FHIR (instâncias). Por exemplo, o registro de uma assistência pode incluir os dados do profissional de saúde, a especialidade, o estabelecimento de saúde onde ocorreu a assistência, além das informações clínicas produzidas na ocasião, dentre outras. Em linhas gerais, a informação para assinatura pode advir de uma ou mais instâncias de recursos FHIR. No segundo caso, quando múltiplos recursos são assinados conjuntamente, é requerido um mecanismo de identificação destes recursos e da ordem em que devem ser considerados.

Vinculação semântica via recurso Provenance. A vinculação semântica da assinatura ao evento clínico registrado é representada pelo recurso Provenance. A

assinatura é fornecida pelo elemento Provenance.signature, que permite identificar o responsável pela assinatura, o instante de criação e outros atributos criptográficos. Essa associação permite identificar a autoria e o contexto operacional da assinatura dentro do ecossistema FHIR.

4 DISCUSSÃO

A definição da política de assinatura digital para o cenário de informação em saúde registrada por meio de instâncias de recursos FHIR inclui regras de como a assinatura deve ser criada e validada. Isso inclui o tipo de certificado digital, algoritmos, regras de canonicalização, formato da assinatura e outros.

Dentro desse contexto, a Figura 2 se refere ao caso de uso *gerar assinatura digital*, e representa uma condensação operacional da política: se refere ao fluxo completo de preparação, transformação, vinculação e criptografia do conteúdo FHIR, apresentando, em uma sequência lógica, cada dependência de dados que leva da entrada do documento ao artefato de assinatura incorporado ao recurso final.

A Figura 2 define as operações necessárias e as relações entre elas para produzir assinaturas digitais conforme a política aqui definida. A política estabelece requisitos ou o arcabouço normativo que orienta implementadores, garante conformidade técnica e sustenta a rastreabilidade de registros da saúde.

As subseções a seguir apresentam de forma estruturada os componentes do caso de uso *gerar assinatura digital*, que compõem a política de assinatura digital proposta.

4.1 Dados de entrada para a geração de assinatura

A Figura 3 ilustra as entradas (E1 a E8) necessárias à efetividade do caso de uso "gerar assinatura digital", para produzir uma assinatura em conformidade com a política de assinatura digital em proposição. Em termos arquiteturais, essas entradas delimitam simultaneamente o conteúdo assinado, o contexto semântico da assinatura, a base criptográfica da confiança e as restrições normativas do processo.

E1 e E2 são as entradas que definem o núcleo documental da assinatura. A Entrada E1 corresponde a uma instância do recurso *Bundle*, serializada em JSON, contendo o conjunto de instâncias FHIR que compõem o conteúdo a ser assinado. Por sua vez, a Entrada E2 representa informações autodeclaradas, tais como autor e contexto da assinatura, e corresponde a uma instância do recurso *Provenance*, também serializada em JSON, na qual deve existir uma entrada em *Provenance.target* para cada instância do conjunto assinado. Vale ressaltar que a ordem em que os recursos são referenciados em *Provenance.target* deve ser preservada, pois essa ordenação participa da determinação exata do conteúdo assinado. Noutras palavras, o par *Bundle-Provenance* implementa a ligação entre a materialidade computacional do documento clínico e as informações autodeclaradas da assinatura, permitindo que a assinatura recaia sobre um conjunto FHIR explicitamente identificado e referenciado, viabilizando a etapa posterior de validação.

As Entradas E3 e E4 tratam da infraestrutura de confiança. A Entrada E3 reúne o material criptográfico do signatário, isto é, a chave privada e/ou as informações necessárias para recuperá-la ou para acionar um serviço externo de assinatura. A Entrada E4, por sua vez, corresponde à cadeia de certificados, indispensável para a validação da confiança, da emissão e da validade temporal do certificado utilizado. Assim, E3 provê a capacidade efetiva de assinar, enquanto E4 provê a base verificável que legitima essa operação perante a infraestrutura de certificação, condição necessária para que a assinatura seja posteriormente validada como tecnicamente íntegra.

A Entrada E5 é o *timestamp* de referência, utilizado em verificações de validade temporal. A Entrada E6 define a estratégia temporal, que indica o uso de carimbo de tempo ou não. A Entrada E7 identifica a política de assinatura digital por meio de uma URI canônica versionada, vinculando a assinatura a uma versão normativa específica. Por fim, a Entrada E8 inclui configurações operacionais que controlam a execução do processo de geração de assinatura.

4.2 Etapas de processo para a política de assinatura digital

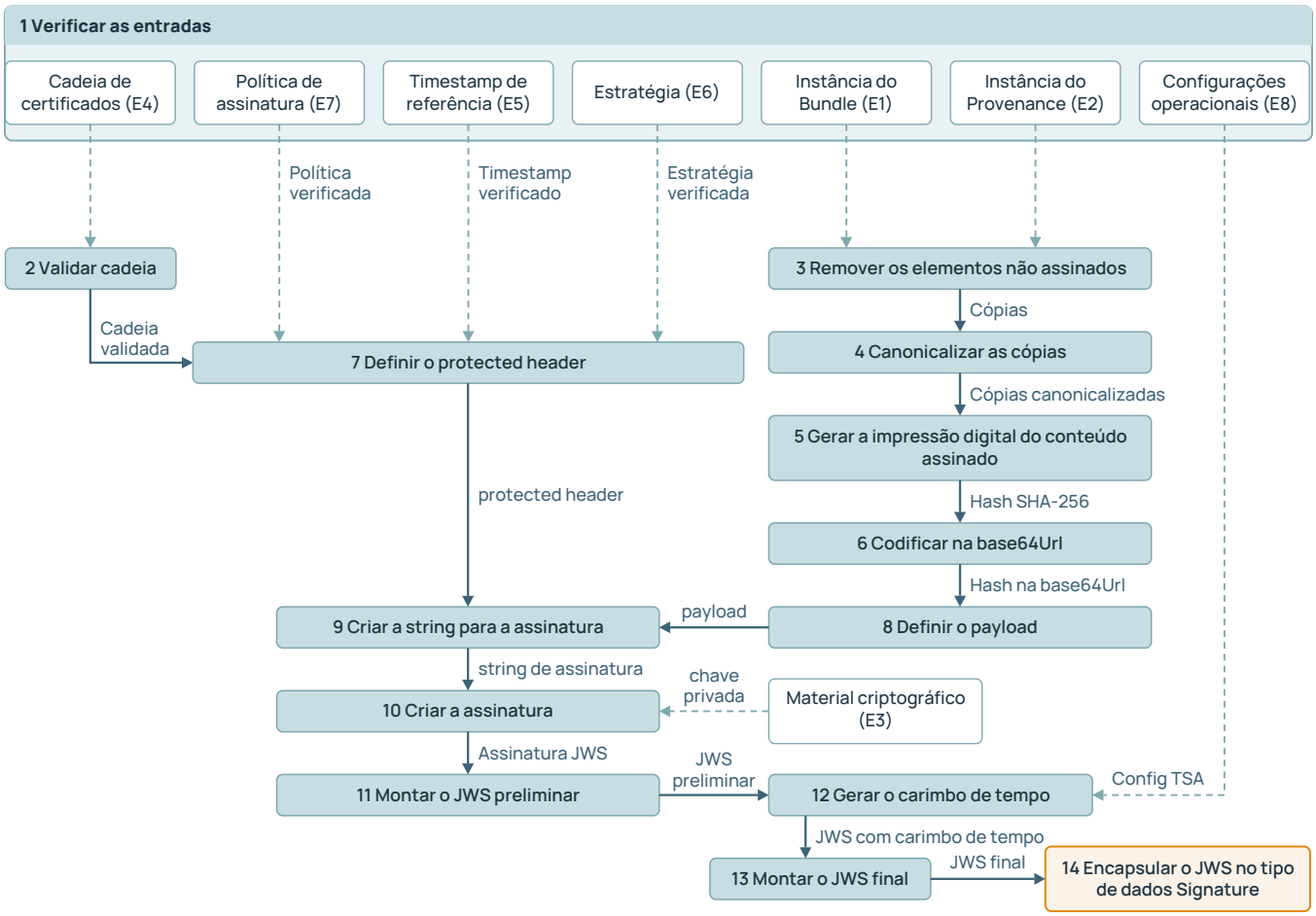
Esta seção apresenta uma descrição conceitual e funcional para cada uma das 14 etapas do processo para a política de assinatura digital. A descrição inclui como as etapas se relacionam com aspectos de segurança, integridade e interoperabilidade no ecossistema FHIR. As etapas são apresentadas na sequência em que são executadas para a geração da assinatura digital, conforme numeradas na Figura 2.

Etapa 1: Verificar as entradas. O processo inicia com uma validação de todas as entradas do processo: *Bundle* (E1), *Provenance* (E2), material criptográfico (E3), cadeia de certificados (E4), *timestamp* de referência (E5), estratégia de validade temporal (E6), política de assinatura (E7) e configurações operacionais (E8). Essa validação busca garantir que todos os elementos requeridos para a assinatura existam, estejam completos e coerentes entre si no contexto FHIR. Tecnicamente, esse passo confere integridade de pré-condição, evitando iniciar um *pipeline* criptográfico com parâmetros inconsistentes.

Etapa 2: Validar cadeia. Uma cadeia é válida se o certificado do assinante é autêntico, não revogado, emitido por uma autoridade confiável (ICP-Brasil) e adequado ao propósito de assinar. O sistema confirma se o certificado do signatário é confiável, se a cadeia

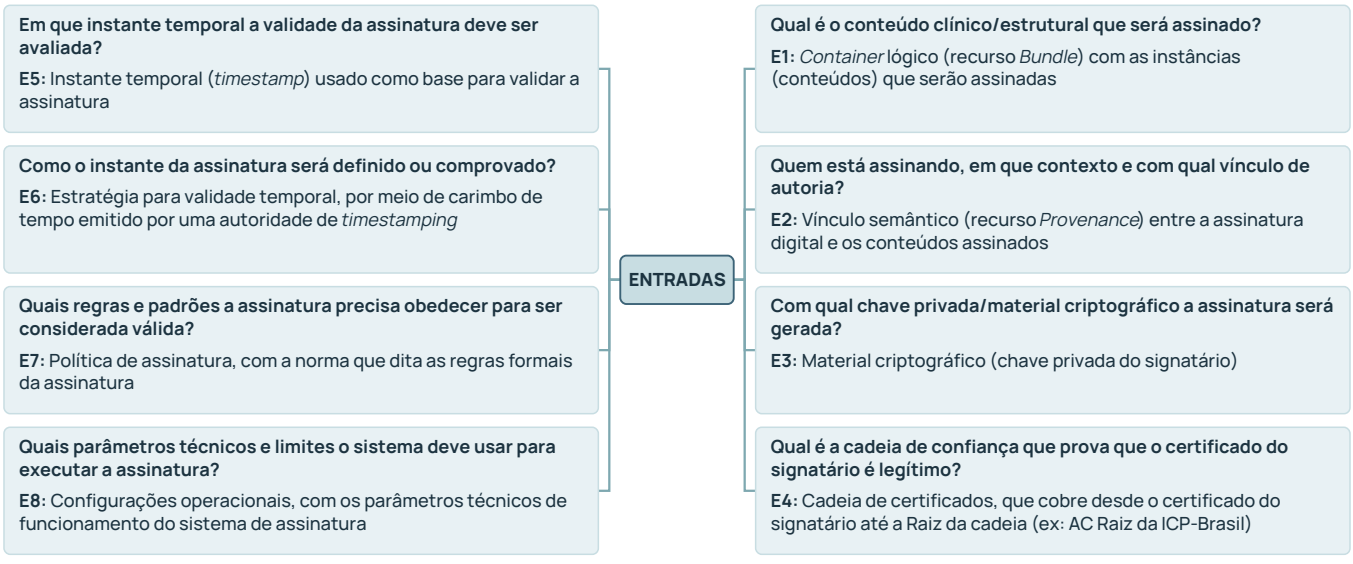
está completa, se os certificados intermediários são válidos, se não há revogação e se os parâmetros de chave correspondem ao algoritmo de assinatura a ser usado. Essa etapa corresponde à verificação X.509 conforme RFC 5280 [11], e garante confiança no emissor

Figura 2. Geração de assinatura digital a partir da Política de Assinatura Digital no ecossistema FHIR.



Fonte: Elaborado pelos autores (2026).

Figura 3. Entradas previstas (E1 a E8) ao caso de uso gerar assinatura digital.



Fonte: Elaborado pelos autores (2026).

da chave privada usada na assinatura.

Etapa 3: Remover elementos não assinados. A instância do recurso *Bundle* pode conter dados que não devem fazer parte do conteúdo a ser assinado, tais

como anexos, metadados e extensões. Nesta etapa, o *pipeline* filtra e replica (gera uma cópia do conteúdo a ser assinado) somente os elementos que serão canonicamente representados para assinar. Noutras palavras, remove-se o que não é parte da verdade clínica, mantendo apenas o conteúdo que deve ser protegido.

Etapa 4: Canonicalizar as cópias. Canonicalizar significa transformar as cópias filtradas em uma representação determinística: ordenação lexicográfica de campos, normalização de espaços em branco, remoção de variações estruturais e serialização conforme regras de canonicalização FHIR/JSON. A ideia é transformar todas as variações possíveis em uma única forma canônica. Tal assegura que um documento terá a mesma representação binária independentemente do servidor, da ferramenta ou do formato JSON adotado. Dessa forma, ao reconstruir um *Bundle* no processo de validação da assinatura, será obtido o mesmo valor de *hash*.

Etapa 5: Gerar a impressão digital do conteúdo assinado. Nesta etapa, as cópias canonicalizadas são submetidas ao cálculo de *hash*, ou seja, é gerado um valor resumido (valor *hash*) pertinente ao conteúdo a ser assinado. O valor *hash* funciona como uma "impressão digital" criptográfica. Nesse contexto, SHA-256 é um algoritmo amplamente utilizado para gerar esses resumos em sistemas críticos [12]: a função *hash* gerará sempre um valor *hash* de 256 bits, independentemente do tamanho do conteúdo a ser assinado; nesse sentido, o valor *hash* é também conhecido como valor resumido ou *digest*. Essa etapa é a espinha dorsal da garantia de integridade: se houver qualquer modificação no conteúdo a ser assinado, o valor *hash* mudará completamente. Em vez de a assinatura ser aplicada diretamente no documento, a assinatura é aplicada no valor *hash*, o que aumenta eficiência e segurança.

Etapa 6: Codificar na Base64Url. A impressão digital gerada (valor *hash*) é codificada em Base64Url [13], para garantir que a informação possa trafegar pela Internet mesmo contendo caracteres reservados (como + ou /), mantendo assim compatibilidade com URLs, HTTP e APIs REST. A codificação em Base64Url permite compatibilidade com o formato JWS conforme especificado em RFC 7515 [14], que foi o formato adotado na política para a assinatura digital. O formato JWS define que a assinatura digital é composta em três partes: *header* (como interpretar a assinatura), *payload* (o valor *hash* do conteúdo canonicalizado que será assinado) e *signature* (resultado do cálculo criptográfico sobre o *header* e o *payload*).

Etapa 7: Definir o protected *header*. O *protected header* é o *header* previsto no formato JWS, e seu conteúdo deve ser imutável: qualquer manipulação posterior à geração da assinatura invalidaria a assinatura. O *header* é a "assinatura da assinatura": explica ao mundo como interpretar e validar a assinatura digital. Seu conteúdo inclui algoritmo, parâmetros críticos, política de assinatura e metadados que influenciam a segurança.

Etapa 8: Definir o *payload*. A função desta etapa é representar o conteúdo clínico que está sendo assinado, ou seja, definir o componente *payload* previsto no formato JWS. A política de assinatura proposta estabelece que o *payload* é representado pelo valor *hash* obtido a partir dos dados canonicalizados. Dessa forma, o algoritmo SHA-256 gerará o *payload* com 256 bits de comprimento para representar o conteúdo clínico, independentemente do tamanho real desse conteúdo.

Etapa 9: Criar a *string* para assinatura. O padrão JWS define formalmente que a *string* para assinatura é a concatenação *header* e *payload*, que cria uma ligação indissociável entre ambos. Essa etapa produz exatamente o material que será criptograficamente protegido, garantindo que *header* e *payload* não possam ser modificados independentemente. É um elo essencial para impedir ataques de substituição (*header swapping*).

Etapa 10: Criar a assinatura. A *string* criada na Etapa 9 é assinada usando a chave privada contida no material criptográfico do signatário, que prova que o documento foi aprovado pelo titular da chave. Essa etapa é o ponto mais sensível de todo o fluxo para garantia de autenticidade e não repúdio. O algoritmo de assinatura digital aplicado é RSA-SHA256, o qual combina o sistema de chaves assimétricas RSA e a função de *hash* SHA-256. O resultado é um conteúdo codificado em *Base64Url* que representa a assinatura digital (a assinatura RSA-SHA256 produz um valor tipicamente com ~300 bytes codificados).

Etapa 11: Montar JWS preliminar. Neste ponto, os três componentes previstos no formato JWS estão disponíveis: *protected header*, *payload* e assinatura. Esses elementos são montados formando um objeto JWS completo, mas ainda sem o registro de *timestamp*. Ao final, é criada uma estrutura JWS preliminar em formato JSON.

Etapa 12: Gerar o carimbo de tempo. Um carimbo de tempo via TSA (*Time Stamping Authority*) é aplicado à assinatura criptográfica, garantindo prova verificável do momento em que a assinatura foi gerada. O carimbo produz uma evidência temporal imutável, assegurando que a assinatura existia naquele momento específico e que os certificados estavam válidos naquela data e hora.

É também criado um bloco de metadados não protegido criptograficamente (*unprotected header*), para anexar informações auxiliares que precisam trafegar junto da assinatura, mas que não estavam disponíveis no momento da assinatura criptográfica primária. O uso de *unprotected header* permite adicionar o carimbo de tempo TSA e evidências de revogação (LTV, *Long*

Term Validation), sem invalidar a assinatura criptográfica já criada, conforme especificação *JAdES*.

Etapa 13: Montar o JWS final. O conteúdo do *unprotected header* é adicionado ao JWS corrente, o que torna a assinatura autossuficiente (autocontida) para validação futura, mesmo que os serviços de rede estejam *offline*.

Etapa 14: Encapsular o JWS no tipo de dados *Signature*. Na etapa final, o artefato JWS JSON é serializado e inserido no elemento *data* do recurso *Signature* do FHIR. Metadados adicionais, como o identificador do signatário (CPF/CNPJ extraído do certificado) e o propósito da assinatura (autoria ou validação), são preenchidos para garantir interoperabilidade total no ecossistema de saúde.

O encadeamento dessas quatorze etapas estabelece um fluxo completo e verificável para a criação de assinaturas digitais aplicadas a recursos FHIR. A partir desse encadeamento, a política de assinatura produz um objeto assinado que pode ser validado em qualquer ponto do ecossistema FHIR, preservando a rastreabilidade dos elementos assinados e a capacidade de comprovar autoria, integridade e temporalidade ao longo de todo o ciclo de vida do documento clínico.

5 CONCLUSÕES

Este trabalho define uma política para a assinatura digital em ecossistemas FHIR, visando à garantia da autenticidade, integridade e não repúdio, por meio de uma especificação implementável da política. O trabalho aplica o método DSR, que sistematiza com rigor a redução de ameaça à validade. A política atende às orientações oficiais HL7 sobre assinaturas digitais, e é orientada a diretrizes abstraídas a partir de publicações científicas recentes.

A política aplica requisitos criptográficos com elementos nativos do FHIR, conforme diretrizes oficiais HL7, especificamente os recursos *Bundle* e *Provenance*, e o tipo de dados *Signature*, como também segue um processo de assinatura posto em 14 etapas, buscando coesão de propósito em cada etapa e alcance de uma assinatura reproduzível e verificável.

Como trabalho futuro, ressalta-se a condução de uma validação robusta da política de assinatura digital, que está em fase preliminar, englobando os seguintes aspectos: conformidade (se a política atende a requisitos tácitos de qualidade, tais como segurança e simplicidade); segurança jurídica (se a política é juridicamente válida em território nacional); alinhamento (se a validação está em linha com o processo de geração); equivalência (se a política possui segurança equivalente ou superior a outras implementações de referência ou similares, caso estejam disponíveis).

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

Agradecimentos. Esta pesquisa é fruto de uma colaboração entre a Secretaria de Saúde do Estado de Goiás (SES-GO) e a Universidade Federal de Goiás (UFG), com foco em interoperabilidade em saúde e em educação continuada. Agradecemos a ambas as instituições pelo suporte ao presente manuscrito.

Financiamento. Os autores não declararam fonte de financiamento.

Disponibilidade de dados e materiais. A estrutura e a semântica completas estão totalmente definidas e disponíveis publicamente em https://fhir.saude.go.gov.br/r4/seguranca/ (fornecido pela Secretaria de Saúde do Estado de Goiás). Este local fornece todos os metadados, ValueSets, perfis e assim por diante.

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

Declaração de uso de IA. A ferramenta Gemini foi utilizada de forma limitada na etapa de revisão final do manuscrito, para a melhoria de fluidez e a precisão linguística do texto. Não houve redução, ampliação ou reestruturação de conteúdo nesses casos.

REFERÊNCIAS

1. Felisberto M, de Oliveira JMD, Mohr ETB, Celuppi IC, Zanotto WL, dos Santos RA, et al. Digital signatures in electronic health records: a scoping review. Health Technol. 2024;14(6):1083-96. doi: https://doi.org/10.1007/s12553-024-00906-y
2. HL7 FHIR. Digital Signatures. 2026. Disponível em: https://build.fhir.org/branches/jdlnolen-FHIR-55280/signatures.html [acessado em Mai/2026].
3. HL7 FHIR. Digital Signatures [Internet]. 2023 [citado 2026 out 18]. Disponível em: https://hl7.org/fhir/R5/signatures.html
4. HL7 FHIR. Implementation Guide: Da Vinci Clinical Data Exchange. 2024. Disponível em: https://build.fhir.org/ig/HL7/davinci-ecdx/signatures [acessado em Mai/2026].
5. HL7 FHIR. Guia de Implementação: SES-GO - Segurança. 2024. https://fhir.saude.go.gov.br/r4/seguranca [acessado em Mai/2026].
6. Baskerville R, Baiyere A, Gergor S, Hevner A, Rossi M. Design Science Research Contributions: Finding a Balance between Artifact and Theory. JAIS. 2018;19(5):358-76. doi: https://doi.org/10.17705/1jais.00495

7. Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S. A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems. 2007;24(3):45-77. doi: https://doi.org/10.2753/mis0742-1222240302

8. HL7 FHIR. FHIR Release 4: Signature Datatype. 2019. Disponível em: https://r4.fhir.space/datatypes.html#Signature [acessado em Mai/2026].

9. Margheri A, Masi M, Miladi A, Sassone V, Rosenzweig J. Decentralised provenance for healthcare data. Int J Med Inform. 2020;141:104197. doi: https://doi.org/10.1016/j.ijmedinf.2020.104197

10. Severo L, Martina J. Digital Medication Prescription System with JSON. In: Proceedings of the 18th International Joint Conference on Biomedical Engineering Systems and Technologies. [s.l.]: SCITEPRESS - Science and Technology Publications; 2025. p. 834-43. doi: https://doi.org/10.5220/0013315700003911

11. Orlando S, Barenghi A, Pelosi G. Investigating the Health State of X.509 Digital Certificates. In: 2024 IEEE International Conference on Cyber Security and Resilience (CSR). [s.l.]: IEEE; 2024. p. 222-7. doi: https://doi.org/10.1109/csr61664.2024.10679412

12. Wu J, Zhang J, Liu D, Wang X. A Multiple-Medical-Image Encryption Method Based on SHA-256 and DNA Encoding. Entropy (Basel). 2023;25(6):898. doi: https://doi.org/10.3390/e25060898

13. Siriwardena P. Base64 URL Encoding. In: Advanced API Security. Berkeley, CA: Apress; 2020. p. 397-9. doi: https://doi.org/10.1007/978-1-4842-2050-4_20

14. Jones M, Bradley J, Sakimura N. JSON Web Signature (JWS). [s.l.]: RFC Editor; 2015. doi: https://doi.org/10.17487/rfc7515

NOTAS EDITORIAIS

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

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