Capítulo 4

Padrões e Soluções para Armazenamento, Compartilhamento e Estruturação de Dados em Saúde Digital: Privacidade, Integração e Desafios

Nicollas R. de Oliveira (UFF), Yago de R. dos Santos (UFF),
Ana Carolina R. Mendes (UFF), Guilherme N. N. Barbosa (UFF),
Marcela T. de Oliveira (TU Delft), Rafael Valle (RNP),
Dianne S. V. Medeiros (UFF), Diogo M. F. Mattos (UFF)

Resumo

A pandemia de COVID-19 enfatizou a necessidade de serviços de saúde ágeis com trocas de informações confiáveis e seguras. O compartilhamento adequado, privado e seguro de Registros Médicos Eletrônicos (Electronic Medical Records – EMRs) é um desafio devido à diversidade de formatos de dados e à fragmentação dos registros em diversos silos de dados. Registros fragmentados atrapalham e atrasam a coordenação entre equipes de saúde, podendo resultar em erros médicos e atrasar o tratamento dos pacientes. O acesso seguro e padronizado aos EMRs tende a melhorar o atendimento ao paciente. Contudo, sistemas de EMR centralizados apresentam riscos à privacidade, enquanto a diversidade de formatos de dados dificulta a interoperabilidade. A tecnologia de cadeia de blocos (blockchain) oferece armazenamento descentralizado, integridade de dados e controle de acesso, eliminando intermediários e aumentando a eficiência. Este capítulo explora padrões de EMR, desafios de segurança e soluções baseadas em cadeia de blocos para interoperabilidade e compartilhamento seguro de dados na área da saúde.

4.1. Introdução

O setor da saúde é um exemplo típico de onde o compartilhamento de dados pessoais entre organizações é essencial e o acesso a esses dados é intrinsecamente distribuído. Os profissionais de saúde de várias organizações precisam analisar os dados dos pacientes para realizar suas tarefas, mas normalmente esses dados estão armazenados em silos localizados em diversos locais e em formatos distintos, dificultando o compartilhamento.

Este capítulo foi realizado com recursos do CNPq, CAPES, RNP, FAPERJ, FAPESP (2018/23062-5) e Prefeitura de Niterói/FEC/UFF (Edital PDPA 2020).

Assim, a complexidade do sistema médico impede que todo o histórico médico do paciente seja facilmente acessado quando necessário. Dessa forma, muita informação é perdida ou exaustivamente repetida, dificultando o diagnóstico e o tratamento do paciente e prejudicando a jornada do paciente.

De acordo com uma pesquisa realizada no Hospital American Johns Hopkins, os erros médicos são a terceira principal causa de morte nos Estados Unidos e a maioria dos erros decorre de problemas sistêmicos, incluindo cuidados mal coordenados [Makary e Daniel, 2016]. O desafio da coordenação dos cuidados aos pacientes pode ser mitigado através do compartilhamento correto e seguro dos dados desses pacientes, permitindo que as equipes possam acessar o histórico completo de saúde do paciente, inclusive para promover o diagnóstico precoce, melhorando a efetividade do tratamento. Ambientes de saúde informatizados facilitam o acesso a esses dados distribuídos, pois os dados do paciente são armazenados sob a forma de Registros Médicos Eletrônicos (*Electronic Medical Records* – EMRs) padronizados. Os EMRs contêm informações pessoais privadas sobre o paciente, incluindo diagnósticos e tratamentos, e normalmente estão distribuídos entre hospitais e clínicas que já trataram o paciente pelo menos uma vez durante sua vida. Os EMRs possibilitam monitorar e acessar de forma rápida e padronizada os dados dos pacientes e permitem integrar o cuidado ao paciente entre os membros da equipe médica e de outras equipes e estabelecimentos de saúde. Assim, possibilita-se que diferentes níveis de atendimento acessem às informações médicas relevantes de cada paciente. Por um lado, o compartilhamento dessas informações é benéfico para o paciente, visto que auxilia a equipe a obter um diagnóstico mais assertivo e, portanto, um tratamento mais adequado para o paciente. Por outro lado, as informações privadas do paciente armazenadas nos EMRs são altamente confidenciais e sensíveis. Essas informações são frequentemente compartilhadas, sem o consentimento do paciente, entre entidades não confiáveis, como profissionais de saúde, farmácias, familiares de pacientes e outros médicos [Dubovitskaya et al., 2017]. Esse compartilhamento é realizado, por exemplo, no momento do encaminhamento de um paciente de uma clínica para um hospital que possua mais recursos para o seu tratamento. Quando possível, os dados do paciente são compartilhados por meio de sistemas médicos institucionais seguros. Contudo, por simplicidade e imediatismo, os dados também são compartilhados por meios de comunicação não institucionalizados e, normalmente, inseguros.

No contexto pandêmico, ressaltou-se a necessidade de tornar mais ágeis os atendimentos e o fluxo de troca de informações entre pacientes, médicos e organizações de saúde. Diante disso, registros dos pacientes adquiriram uma maior importância em termos de saúde pública [Stoeger e Schmidhuber, 2020] e dados sobre diagnósticos e medicamentos prescritos podem ser utilizados para identificar pessoas em grupos de risco da COVID-19, por exemplo. A maior disponibilidade de dados dos pacientes em formato eletrônico é de grande relevância para a tomada de decisão e continuidade do cuidado nos setores público e privado, principalmente com troca de informações entre as duas esferas. Dados que indiquem precocemente focos de surtos de doenças são importantes para coordenar ações de políticas de saúde pública para prevenção em âmbito nacional e de forma eficiente. Os benefícios do compartilhamento eficiente estendem-se aos pacientes também, uma vez que permite que os pacientes acessem suas próprias informações a qualquer momento, tais como resultados de exames laboratoriais e de imagens, sendo

possível realizar a portabilidade desses dados para outro médico ou organização de saúde. A comunicação eficiente e automatizada entre os pacientes e as equipes médicas [Hurst et al., 2022] universaliza o acesso aos dados promovendo transparência e um aumento da satisfação do paciente.

A importância e a relevância da disponibilidade de dados são crescentes e essa disponibilidade está sendo implementada em muitos estabelecimentos. Em 2019, por exemplo, verificou-se um aumento na disponibilidade de informações do paciente em formato eletrônico. Entre os principais aumentos em relação a 2018 estão: dados cadastrais dos pacientes (89% contra 79%); principais motivos que levaram o paciente à consulta (64% contra 50%) e admissão, transferência e alta (56% contra 43%) [Cetic.br, 2020]. Quanto às funcionalidades do sistema eletrônico, o destaque é o aumento de sua disponibilização nos estabelecimentos públicos nos últimos anos, principalmente em relação a listar todos os resultados de exames laboratoriais (de 17%, em 2016, para 41%, em 2019), listar todos os pacientes que usam uma medicação (de 18%, em 2016, para 40%, em 2019) e realizar prescrição médica (de 29% para 51%) [Cetic.br, 2020]. Esses aumentos podem indicar uma evolução no nível e na complexidade dos sistemas eletrônicos adotados, que resultam em menor fragmentação na prestação do cuidado, favorecendo a qualidade e eficiência, e reduzindo lacunas no atendimento [Janett e Yeracaris, 2020]. No entanto, avanços na adesão de práticas de digitalização de dados e o consequente aumento significativo nos dados sensíveis gerados, expõe diversos desafios a serem abordados pelos sistemas.

Atualmente, os sistemas de EMR baseiam-se majoritariamente em arquiteturas cliente-servidor centralizadas, nas quais uma autoridade central possui acesso completo ao sistema. Todavia, essa arquitetura apresenta alguns desafios relacionados à privacidade e à segurança. Vulnerabilidades no sistema podem resultar em falhas e criar brechas para invasores cibernéticos comprometerem os dados do paciente [Tanwar et al., 2020]. O gerenciamento desses sistemas impõe um desafio para preservar a privacidade enquanto garante a disponibilidade de dados para os agentes autorizados. Paralelamente, os registros são frequentemente mantidos de forma fragmentada em bancos de dados locais, o que impede que um paciente tenha um prontuário eletrônico consolidado [Mettler, 2016].

A padronização do formato de dados é imprescindível para permitir a interoperabilidade na área da saúde. A padronização envolve o estabelecimento de uma linguagem comum para a troca e interpretação de dados médicos, permitindo que sistemas diferentes se comuniquem. No entanto, alcançar essa padronização é um desafio, pois à medida em que o número de aplicativos de saúde, EMRs e dispositivos médicos continuam a se multiplicar, a diversidade de formatos de dados prolifera exponencialmente. Essa fragmentação apresenta desafios significativos para profissionais de saúde, pesquisadores e formuladores de políticas que buscam aproveitar o poder dos dados para melhorar o atendimento ao paciente, avanços em pesquisas e tomadas de decisão baseadas em evidências.

A tecnologia de cadeia de blocos (*blockchain*) apresenta-se como uma tendência para a padronização e interoperabilidade de registros médicos eletrônicos, visando permitir que o EMR seja verificado e registrado por meio de um consenso de pares que participam de uma rede par-a-par, garantindo a execução confiável de políticas de acesso aos dados e, portanto, assegurando integridade dos dados, responsabilidade e não-repúdio [Christidis e Devetsikiotis, 2016]. Em suma, a tecnologia de cadeia de blocos

torna-se naturalmente atrativa no desenvolvimento de aplicações que (i) exigem a contribuição de várias partes interessadas, embora a confiança entre as partes seja complexa de ser fornecida com tecnologias atuais, (ii) carecem de um rastreamento confiável de atividade e confiabilidade de dados e (iii) desejam remover partes intermediárias, aumentando a eficiência geral do sistema [Engelhardt, 2017]. Nesse contexto, o setor de saúde surge como um candidato no qual a tecnologia de cadeia de blocos tem o potencial de desempenhar um papel fundamental, principalmente devido aos seguintes elementos-chave [Siyal et al., 2019, Namasudra et al., 2022]:

- **Descentralização:** não há necessidade de intermediário e o sistema de banco de dados está disponível para qualquer pessoa conectada à rede que possua o nível de acesso necessário. O monitoramento, armazenamento, acesso e atualização de dados podem ser realizados nos diversos sistemas que fazem parte da rede;

- **Transparência:** os dados registrados e armazenados em uma cadeia de blocos são transparentes para os usuários, ou seja, todos os usuários podem visualizar as transações realizadas via cadeia de blocos;

- **Imutabilidade**: os dados armazenados não podem ser modificados, permitindo que os interessados provem com certeza matemática que o fluxo de dados históricos é exato e não modificado [Engelhardt, 2017];

- **Autonomia:** os nós da rede são independentes e autônomos, podendo acessar, transferir, armazenar e atualizar dados com segurança e sem intervenção externa;

- **Anonimato:** a identidade dos participantes é anônima, contribuindo para a privacidade, segurança e confiabilidade do sistema.

Este capítulo apresenta os principais padrões de armazenamento e compartilhamento de registros médicos eletrônicos. Os padrões, desde os tradicionais padrões *Health Level 7* (HL7) e Imagem Digital e Comunicações em Medicina (*Digital Imaging and Communications in Medicine* – DICOM) até formatos emergentes como Recursos Rápidos de Interoperabilidade de Assistência Médica (*Fast Healthcare Interoperability Resources* – FHIR) e Registro Eletrônico de Saúde Aberto (*Open Electronic Health Record* – openEHR), são apresentados em domínios de uso específicos, tais como armazenamento, compartilhamento, estrutura e terminologias. São abordados os principais desafios de segurança e privacidade no acesso aos dados médicos, focando mecanismos de controle de acesso disponíveis em plataformas de uso comercial e de código aberto. Esses desafios incluem modelos de dados incompatíveis, terminologia e sistemas de codificação variados, práticas de implementação divergentes, desafios de privacidade e de segurança, e da necessidade de políticas e regulamentos harmonizados entre diferentes domínios de validade dos dados de saúde. O capítulo discute o controle de acesso aos dados médicos e foca propostas que visam o uso da tecnologia de cadeia de blocos para o compartilhamento de dados e gerência de políticas de acesso. O capítulo também apresenta conceitos fundamentais sobre a tecnologia de cadeia de blocos, necessários para o entendimento das propostas que utilizam essa tecnologia. A Figura 4.1 mostra a organização da estrutura

deste capítulo. Aos leitores já familiarizados com os conceitos relacionados à tecnologia de cadeia de blocos, recomenda-se seguir a sequência de seções indicada pelas setas sólidas, sem prejuízo à compreensão do capítulo.

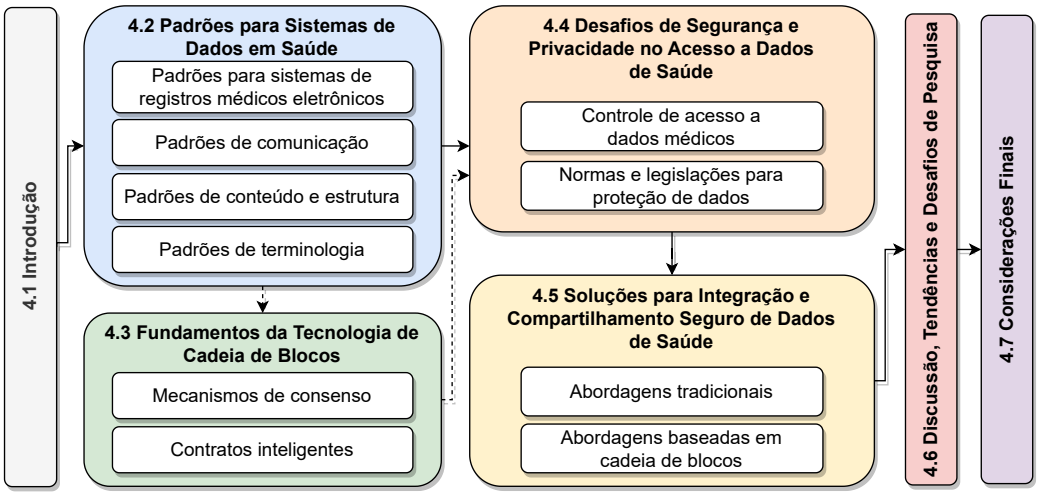

Figura 4.1. Organização da estrutura do minicurso. A sequência de seções indicada pelas setas sólidas é recomendada para os leitores familiarizados com os conceitos básicos relacionados à tecnologia de cadeia de blocos. As setas tracejadas indicam um desvio passando pela Seção 4.3, que apresenta os fundamentos da tecnologia de cadeia de blocos.

4.2. Padrões para Sistemas de Dados em Saúde

Os padrões para sistemas de dados de saúde são formados por conjuntos de normas, especificações e diretrizes que objetivam parametrizar a maneira como as informações clínicas e administrativas são coletadas, armazenadas, processadas e compartilhadas em sistemas de saúde. Além dos padrões para sistemas de saúde, algumas organizações também contribuem para a padronização dos métodos de comunicação entre sistemas, estrutura e normas para armazenamento e representação de dados clínicos, produzindo uma grande variação de padrões para sistemas médicos no mundo. Esta seção aborda padrões de (i) sistemas de registros médicos eletrônicos; (ii) conteúdo e estrutura; (iii) comunicação; e (iv) terminologias. A Tabela 4.1 resume os tipos de padrões abordados nesta seção. No Brasil, existem diversos órgãos responsáveis pela adoção e implementação desses padrões, como o Ministério da Saúde (MS), a Agência Nacional de Saúde Suplementar (ANS), o Conselho Nacional de Secretários de Saúde (CONASS) e o Conselho Nacional de Saúde (CNS). Paralelamente, existem padrões internacionais que são amplamente adotados no desenvolvimento de sistemas em diversos países. O entendimento e seleção desses padrões é fundamental para garantir a interoperabilidade entre os diferentes sistemas de saúde disponíveis no mercado e promover uma assistência à saúde mais eficiente, segura e de qualidade.

4.2.1. Padrões para sistemas de registros médicos eletrônicos

Os padrões de sistemas de registros médicos eletrônicos têm como foco central promover a interoperabilidade entre diferentes sistemas e aplicações de saúde, permi-

Tabela 4.1. Padrões apresentados no capítulo, classificados de acordo com o tipo de padrão e a entidade padronizadora.

Tipo de Padrão	Nome do Padrão	Entidade Padronizadora
Registro médico eletrônico	openEHR (*Open Electronic Health Record*)	openEHR
Conteúdo e estrutura	CDA (*Clinical Document Architecture*)	HL7 (*Health Level 7*)
	FHIR (*Fast Healthcare Interoperability Resources*)	HL7
	DICOM (*Digital Imaging and Communications in Medicine*)	NEMA (*National Electrical Manufacturers Association*)
Comunicação	FHIR	HL7
	HL7 V2 (HL7 *Version 2*)	HL7
	HL7 V3 (HL7 *Version 3*)	HL7
	DICOM	NEMA
Terminologia	TUSS (Terminologia Unificada da Saúde Suplementar)	ANS (Agência Nacional de Saúde), AMB (Associação Médica Brasileira), COPISS (Comitê de Padronização das Informações em Saúde Suplementar)
	SNOMED CT (*Systematized Nomenclature of Medicine - Clinical Terms*)	SNOMED International
	LOINC (*Logical Observation Identifiers Names and Codes*)	Regenstrief Institute
	ICD (*International Classification of Diseases and Related Health Problems*)	OMS (Organização Mundial de Saúde)

tindo o compartilhamento e a troca de informações de saúde de forma segura, eficiente e precisa. Tais padrões fundamentam a formulação de modelos de referência alinhados a leis e regulamentações e dedicados ao desenvolvimento de novas aplicações de saúde.

A **openEHR** é uma das organizações responsáveis pela produção e manutenção de especificações e padrões de sistemas de *software* para registros médicos eletrônicos, que recebem o mesmo nome da organização, *openEHR*. Embora proponha modelos para sistemas de saúde, a organização não possui aplicações próprias, tendo como principal contribuição duas arquitetura de referência focadas na integração entre soluções de *software* de saúde[2], juntamente a especificação de componentes necessários para a implementação da proposta. Além das arquiteturas de referência, a openEHR também especifica os componentes da arquitetura, tanto em relação ao modelo, quanto a aspectos de comunicação, armazenamento, integração e representação dos dados. As especificações *openEHR* utilizam uma abordagem de separação de papéis, atribuindo aos profissionais da saúde a responsabilidade da definição de procedimentos e do primeiro nível de representação dos dados no modelo, que dependem do contexto e são chamados de arquétipos. Paralelamente, designa aos desenvolvedores apenas as funções de integração dos componentes, interface gráfica e serviços de *software* sobre os dados.

A openEHR especifica primeiramente um modelo geral organizado em componentes. Cada componente e suas especificidades são detalhados nas definições do pa-

[2]Disponível em `https://openehr.org/developers`.

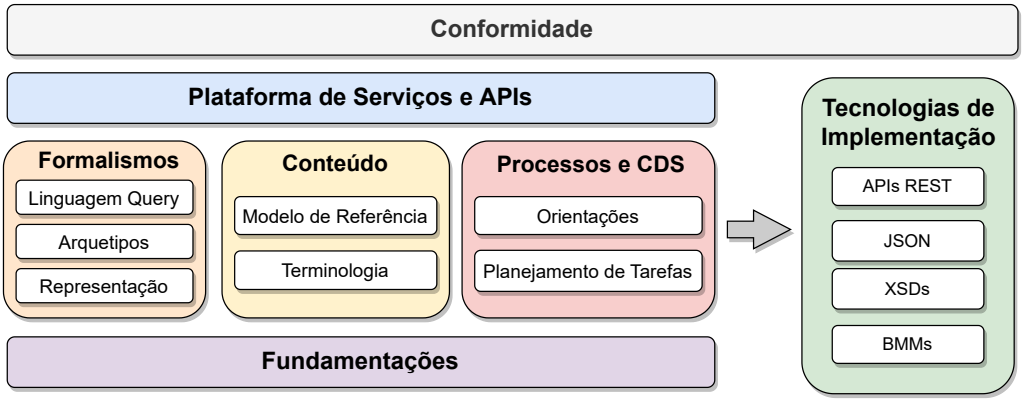

Figura 4.2. Organização dos componentes das especificações dos modelos de referência openEHR.

drão. As duas arquiteturas de referência especificadas pela openEHR são particularizações desse modelo geral. A Figura 4.2 apresenta a organização das especificações em blocos de funcionalidades do modelo geral proposto pela openEHR[3]. Esses blocos são organizados da seguinte forma:

- **Conformidade:** componente dos critérios de conformidade da aplicação modelo, formando um guia para testes de validação do sistema para licitações, das regras de segurança, testes de integração, API etc. Geralmente aplicado sobre as Especificações de Tecnologias de Implementação (*Implementation Technology Specifications* – ITS);
- **Plataformas de Serviços e Interfaces de Programação de Aplicação (*Application Programming Interfaces* – APIs):** define APIs formais abstratas que determinam as interfaces para a plataforma openEHR;
- **Formalismos:** define formalismos genéricos utilizados tanto para consulta de dados quanto para a definição de dados e procedimentos estáticos, incluindo os arquétipos, que são bibliotecas de classes organizadas em contextos médicos de finalidade pré-definida, porém sendo genéricas o suficiente para a reutilização. Além disso, define a biblioteaca de representação das classes internas em Linguagem de Modelagem Unificada (*Unified Modeling Language* – UML) e a Linguagem de Consulta de Arquétipo (*Archetype Query Language* – AQL), que é linguagem *query* de consulta portátil para os arquétipos;
- **Conteúdo:** define modelos de conteúdo primário da plataforma openEHR, incluindo dados demográficos e registros eletrônicos de saúde. Além disso, suporta a terminologia openEHR, juntamente com expressões de outras terminologias.
- **Processos e Suporte à Decisão Clínica (*Clinical Decision Support* – CDS):** define componentes do processo clínico e do CDS, contendo as especificações de planejamento de tarefas e a Linguagem de Definição de Orientações (*Guideline Definition*

[3]Disponível em https://specifications.openehr.org/releases/BASE/latest/architecture_overview.html.

Language – GDL), ambos usados para desenvolver manuais e orientações de uso organizados por contexto nas aplicações. O componente é voltado aos usuários das aplicações;

- **Fundamentações (*Foundation*):** define tipos primitivos, identificadores e outras classes fundamentais para o funcionamento da openEHR;

- **Especificações de Tecnologias de Implementação (ITS):** define componentes das especificações openEHR que focam na interoperabilidade, como API de comunicação e os diversos tipos de codificação de dados, como o Notação de objeto JavaScript (*JavaScript Object Notation* – JSON) e Definição do Esquema XML (*XML Schema Definitions* – XSDs), além da coleção de representação do modelo utilizado para interfacear com outros sistemas, como o Metamodelo Básico (*Basic Meta-Model* – BMM).

A primeira arquitetura de referência da openEHR é um sistema de informação médico genérico. Essa arquitetura propõe servir de base para o desenvolvimento de aplicações com interoperabilidade garantida. Isso é possível porque o modelo define todos os componentes com base em padrões estabelecidos tanto pela openEHR quanto por outros grupos, como a organização HL7, que define padrões de comunicação e estrutura (Seção 4.2.3 e Seção 4.2.2). A utilização de padrões de comunicação facilitam a troca de dados entre sistemas distintos, definindo formatos, arquitetura de documento, elementos de dados, conteúdo, métodos e APIs usados para alcançar a interoperabilidade.

A segunda arquitetura especificada é referência para um sistema de integração entre outros sistemas, funcionando como um *middleware* de padronização na comunicação e armazenamento de dados. O objetivo central é a integração e padronização de sistemas legados. Dessa forma, para essa arquitetura os esforços são concentrados na definição das APIs entre os diferentes sistemas. As especificações viabilizam a captura, armazenamento, recuperação e compartilhamento de informações clínicas em um formato comum.

Devido à natureza dinâmica dos sistemas de saúde, as especificações openEHR são bem detalhadas, porém as arquiteturas e modelos são genéricos. As especificações se limitam em definir o formalismo do arquétipo necessário para expressar o conteúdo de um domínio, por exemplo, através de *templates* e formulários. Além disso, a openEHR define uma interface de programação de aplicação aberta e uma coleção de modelos estáticos pré-definidos, tais como dados demográficos, procedimentos médicos universais e outros recursos úteis para agilizar o processo de desenvolvimento da maioria dos sistemas que focam atender.

4.2.2. Padrões de conteúdo e estrutura

Os padrões de conteúdo e estrutura determinam a estrutura dos documentos eletrônicos e os tipos de dados que esses documentos devem conter. Os padrões de conteúdo focam especificar quais dados dos pacientes devem ser armazenados e de que forma são relacionados com as etapas do atendimento, acrescentando semântica aos documentos, gerando histórico e informações úteis para o tratamento continuado. Em contrapartida, os padrões de estrutura visam garantir o compartilhamento dos dados entre sistemas e

ampliar a interoperabilidade entre unidades de saúde, sem ditar a forma como esses documentos devem ser transmitidos.

O **CDA** é um tipo de documento geralmente representado em XML que contém dados do paciente e o contexto do atendimento. O CDA é desenvolvido e mantido pela organização HL7, um dos mais importantes grupos de padronização para sistemas médicos. Historicamente, os sistemas médicos que adotaram o CDA não detinham uma definição formal de implementação. Então, surgiram algumas variações para a utilização desse padrão. A HL7 agrupou, documentou, especificou e aprimorou as variações existentes, definindo o padrão de implementação para documentos CDA [HL7, 2015]. O padrão CDA define, então, uma biblioteca de referência para documentos CDA. O CDA é especificado tanto no âmbito de conteúdo e estrutura, quanto para casos de uso nos atendimentos, o que torna o padrão menos genérico. Em decorrência disso, o padrão CDA é organizado em *templates* baseados em casos de uso, tendo atualmente 12 especificações distintas. A implementação é orientada a objetos e contém todas as características desse paradigma, sendo adequado para os casos que necessitam de hierarquia.

O **FHIR** é um arcabouço de padrões de próxima geração criado pela HL7[4]. O FHIR tem como foco a padronização da representação e transação de dados de registros médicos eletrônicos, podendo ser entendido como um conjunto de regras e especificações baseados nas principais funcionalidades dos padrões tradicionais desenvolvidos pela organização HL7, como o HL7 Version 2 (HL7 V2), HL7 Version 3 (HL7 V3) e o CDA. Para representar os dados intercambiáveis, o FHIR utiliza um elemento básico chamado Recurso[5]. Cada Recurso é estruturado seguindo o mesmo formato e pode fornecer informações sobre dados demográficos do paciente, diagnósticos, medicamentos, alergias, planos de cuidados, dentre outras informações. Os Recursos são organizados em seções e precisa conter informações sobre o tipo de Recurso, um identificador do Recurso, os metadados do documento, dados humanamente legíveis em XHTML resumindo o documento, uma referência para o tipo de documento na documentação do sistema e os dados padronizados do paciente ou do exame, como número do registro médico, nome do paciente, plano de saúde, identificação da clínica que está emitindo ou consultando o documento, entre outros. Os Recursos podem ser representados nos formatos XML, JSON e RDF. É válido destacar que o FHIR se diferencia do CDA na representação dos dados por não ter limitação de conteúdo como o CDA, que representa apenas informações clínicas. Além disso, o CDA requer o uso de *templates* para suportar a interoperabilidade. Já no FHIR o conteúdo é interpretado de acordo com a definição do tipo de Recurso, sendo necessário haver a definição do Recurso para que o dado possa ser compartilhado. Ademais, o CDA define a própria sintaxe XML fracamente baseada em HTML. Diferentemente, o FHIR usa um conjunto restrito de XHTML que é mais expressivo do que a marcação usada no CDA. A Figura 4.3 mostra um exemplo de um Recurso do FHIR em XML, destacando as seções de estrutura do documento. A primeira seção, bloco verde, contém o identificador do Recurso e sua versão representada em forma de data e hora da última atualização. Na área de resumo, bloco roxo, são apresentadas as informações do recurso em formato XHTML, dando suporte para leitura direta em um navegador *web*. Na seção de definição, em laranja, é representado o Localizador Uniforme de Recursos (*Uniform Resource Lo-*

[4]Disponível em `https://www.hl7.org/fhir/summary.html`.
[5]Disponível em `https://www.hl7.org/fhir/structuredefinition.html`.

cator – URL) da especificação do recurso utilizado. Por fim, os dados do registro com o identificador único do paciente MRN *Medical Record Number*, os dados demográficos e resultados de um exame estão representados no último bloco, em azul. Os URLs para as terminologias de referência para o significados dos valores, utilizando rótulos <*system*> e <*value*>, servem de suporte para a padronização e remoção de ambiguidade dos dados representados.

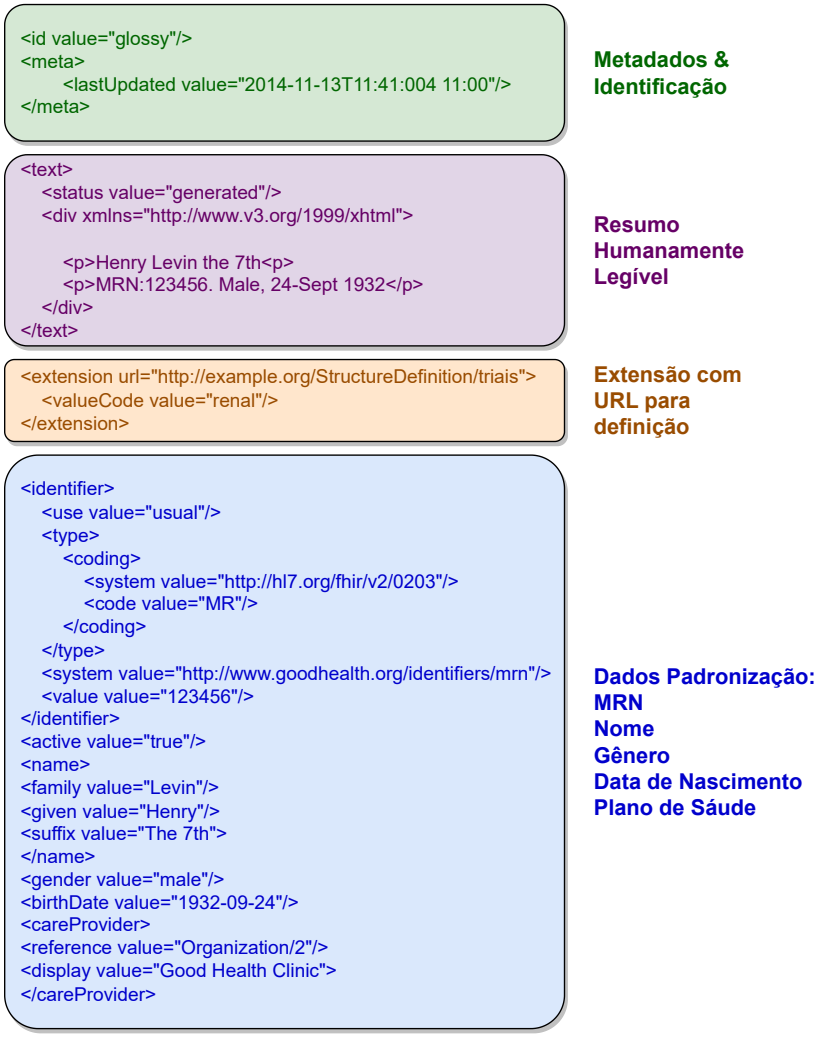

Figura 4.3. Exemplo de um Recurso do FHIR com as seções de estrutura do documento em destaque. A primeira seção, em verde, contém informações sobre metadados e identificação do recurso. A seção seguinte, em roxo, contém o resumo humanamente legível, representado em formato XHTML. A terceira seção, em laranja, contém informações adicionais que não estão na definição básica do tipo de Recurso. A última seção, em azul, contém os dados do registro.

O **DICOM** é um padrão internacional de comunicação, armazenamento e representação de imagens médicas e dados derivados de tomografia computadorizada, ressonância magnética e radiografia, entre outros exames de imagem [DICOM, 2023]. Como os formatos de arquivo de imagem tradicionais (JPEG, TIFF, BMP) não são suficientes para o diagnóstico acurado, o padrão adiciona aos arquivos informações necessárias para fins de diagnóstico, como dados demográficos sobre o paciente, parâmetros de aquisição

para o estudo de imagem, dimensões da imagem, espaço de cores e uma série de informações adicionais para exibir corretamente a imagem no computador. Assim, permite-se a padronização das imagens médicas e dos dados associados, facilitando a interpretação e o diagnóstico pelos profissionais de saúde. A padronização do formato dos arquivos e do método de comunicação possibilita que as mídias sejam compartilhadas através de serviços como Sistema de Arquivo e Comunicação de Imagens (*Picture Archiving and Communication System* – PACS) e Sistema de Informação Radiológica (*Radiological Information System* – RIS), dando aos profissionais da saúde mais recursos para a análise clínica. O padrão foi desenvolvido desde 1983 pelo comitê formado pela Colégio Americano de Radiologia (*American College of Radiology* – ACR) e Associação Nacional de Fabricantes Elétricos (*National Electrical Manufacturers Association* – NEMA), e tem como foco facilitar a interoperabilidade entre equipamentos de imagens médicas. O comitê especifica os protocolos de rede para comunicação que os equipamentos devem utilizar para transportar os dados, a sintaxe e a semântica dos comandos associados à troca de dados no contexto de imagens médicas, um conjunto de definições para serviços de armazenamento das mídias, assim como a especificação de um formato de arquivo próprio e um padrão para a estrutura dos diretórios de armazenamento. Todas essas especificações e definições compõem o escopo do padrão DICOM que são expressadas em forma de classes Par Objeto-Serviço (*Service-Object Pair* – SOP). Essas classes representam serviços, como armazenamento usando rede, mídia ou *web*, operando em tipos de objetos de informação, como imagens tomografia computadorizada ou ressonância magnética. A Figura 4.4 apresenta o modelo geral dos serviços e funções DICOM e suas especificações para transporte dos dados de imagem, suas informações derivadas, comunicação em tempo real e para o acesso aos arquivos diretamente.

4.2.3. Padrões de Comunicação

O **FHIR** foi projetado com foco em implementação com flexibilidade, aproveitando as convenções de comunicação *web* já consolidadas, como representação de dados utilizando JSON, XML e troca de dados através de APIs RESTful baseadas em HTTP. O padrão dá suporte para troca de mensagens e documentos em sistemas desacoplados, ou com arquiteturas orientadas a serviços, indo ao encontro de tendências mais modernas para desenvolvimento de *software* em geral. Os Recursos definidos pelo FHIR são otimizados para a realização de transações sem manutenção de estado por meio de APIs RESTful. Transações desse tipo são as únicas que estão definidas até o momento pela especificação FHIR. As transações seguem um padrão simples de "solicitação" e "resposta". As solicitações e respostas podem ocorrer para obtenção de carga útil individual ou em lote. A carga útil é composta por um cabeçalho e pelo conteúdo de interesse. A leitura de um Recurso, por exemplo, é feita através de uma operação `Read Request` que envia uma solicitação HTTP GET para o URL do Recurso[6].

O **HL7 V2**[7] é um padrão de troca de mensagens no contexto de aplicações médicas, tendo como função principal a definição de padrões para o conteúdo ou corpo das mensagens, protocolo de envio e recebimento de mensagens e definição de contextos va-

[6]Disponível em https://www.hl7.org/fhir/overview-dev.html

[7]Disponível em https://www.hl7.org/implement/standards/product_section.cfm?section=13.

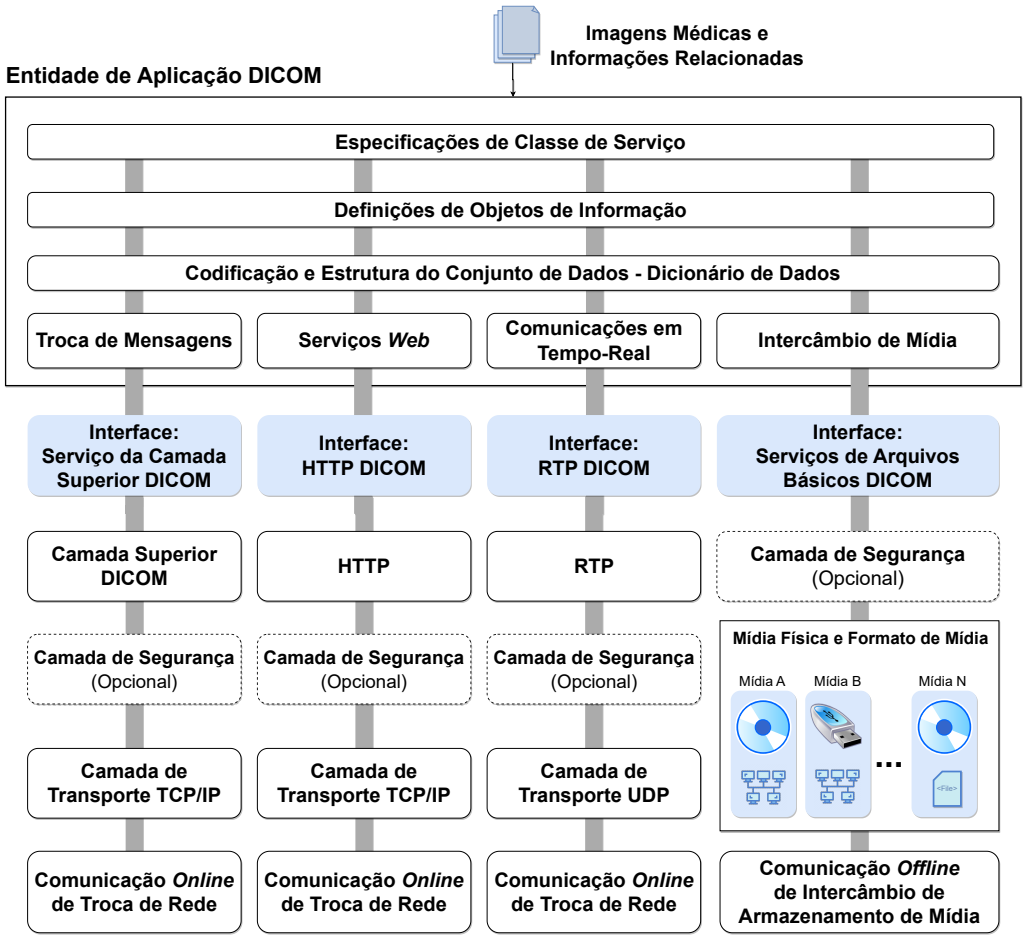

Figura 4.4. Modelo geral dos serviços de armazenamento, disponibilização e tratamento das imagens DICOM, juntamente com as funções para a transação de documentos DICOM, com saída para troca de mensagem, serviços *web* (REST API), transmissão em tempo real e exportação de arquivo para mídias físicas, que fazem parte da aplicação DICOM, geralmente disponibilizada em um servidor *online*. Na parte inferior da figura são apresentados os protocolos de comunicação e transporte especificados para cada tipo de serviço, servindo de base para a integração dos sistemas que consomem os dados da aplicação DICOM.

riados, tais como requisição de histórico, dados demográficos, entre outros. A estrutura de mensageria do HL7 V2 é baseada em um paradigma de mensageria baseada em eventos. O HL7 V2 define a sintaxe da comunicação em baixo nível, sem se preocupar que as mensagens sejam humanamente legíveis, introduzindo todo o conteúdo da mensagem em uma cadeia de caracteres. Os dados são separados por um sinal de barra vertical "|", como mostra a Figura 4.5[8]. Do lado esquerdo existe um identificador do dado e do lado direito o valor. Os identificadores são definidos pelo padrão HL7 V2. Assim, a escolha de quais dados e valores devem estar na mensagem depende do contexto da requisição e do seu respectivo fluxo. A Figura 4.6 apresenta o fluxo de mensagens para transferir informações de imunização de um sistema de informações de saúde para outro. O Sistema Emissor

[8]Disponível em https://www.ringholm.com/docs/04300_en.htm.

pode ser um sistema de EMR, um Sistema de Informações de Imunização (*Immunization Information System* – IIS) ou outro tipo de sistema de informações de saúde. Um evento como uma atualização ou novo registro inserido no Sistema Emissor inicia a criação e envio de uma mensagem VXU (*Vaccination Update*), contendo um registro de imunização atualizado. O Sistema Receptor recebe a mensagem e a processa de acordo com o perfil utilizado, aplicando regras de negócios locais. Após o processamento bem sucedido, o receptor envia uma mensagem de reconhecimento (*Acknowledgement* – ACK) e adiciona o novo registro ao Sistema Receptor [Savage, 2014].

```
MSH|^~\&|GHH LAB|ELAB-3|GHH OE|BLDG4|200202150930||ORU^R01|CNTRL-3456|P|2.4<cr>
PID|||555-44-4444||EVERYWOMAN^EVE^E^^^^L|JONES|19620320|F|||153 FERNWOOD DR.^
^STATESVILLE^OH^35292||(206)3345232|(206)752-121||||AC555444444||67-A4335^OH^20030520<cr>
OBR|1|845439^GHH OE|1045813^GHH LAB|15545^GLUCOSE|||200202150730||||||||
555-55-5555^PRIMARY^PATRICIA P^^^^MD^^|||||||||F||||||444-44-4444^HIPPOCRATES^HOWARD H^^^^MD<cr>
OBX|1|SN|1554-5^GLUCOSE^POST 12H CFST:MCNC:PT:SER/PLAS:QN||^182|mg/dl|70_105|H|||F<cr>
```

Figura 4.5. Exemplo de uma mensagem de resultado de exame de glicose e dados demográficos de um paciente no padrão HL7 V2. Do lado esquerdo do "|" existe um identificador do dado e do lado direito o valor desse dado.

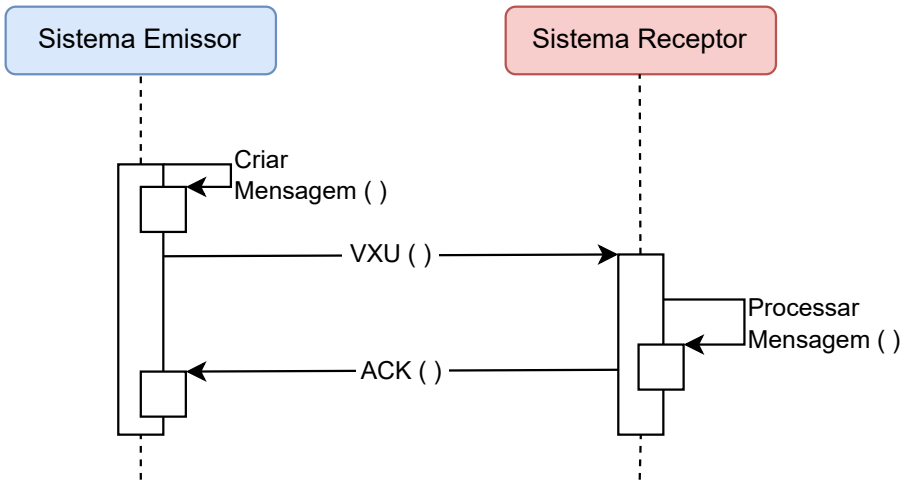

Figura 4.6. Diagrama de sequência da especificação do fluxo de atualização do histórico de imunização de um paciente utilizando o padrão HL7 V2. Adaptado [Savage, 2014].

O **HL7 V3**[9] difere do HL7 V2 ao incorporar um Modelo de Informação de Referência (*Reference Information Model* – RIM) para configurar o formato de mensagens em uma modelagem orientada a objetos. No HL7 V3, as mensagens são codificadas em um mapeamento de classes de informações necessárias para o contexto de aplicações médicas. Cada classe recebe seu Identificador Único de Objeto (*Object Identifier* – OID) para assegurar a universalidade da especificação de cada objeto no seu contexto. As especificações apresentam atributos já conhecidos no HL7 V2, como dados demográficos, relacionamentos e os fluxos de troca de dados como máquinas de estado. Contudo, com a utilização do RIM, o HL7 V3 também ganha especificações para subconjuntos das classes

[9]Disponível em https://www.hl7.org/implement/standards/product_brief.cfm?product_id=186.

do RIM, ou seja, no HL7 V3 as classes são organizadas e reutilizadas para diferentes contextos médicos, sendo isso também parte da especificação do padrão. Consequentemente, o padrão HL7 V3 foi organizado de forma orientada a contexto de uso, ou de especificação de domínio, que são conjuntos de classes do RIM que formam um grupo aplicado a alguma área do domínio dos sistemas médicos, como atendimento, exames, cobrança, atendimento emergencial, conhecidos como Modelo de Informação de Mensagem de Domínio (*Domain Message Information Model* – D-MIM).

Todos os fluxos, protocolos de comunicação e terminologias adotadas para o HL7 V2 dão base para o HL7 V3, que traz como foco especificar a codificação das mensagens utilizando XML e sua sintaxe. Dessa forma, o padrão torna-se mais inteligível e de fácil implementação. A Figura 4.7[10] apresenta um trecho da mesma mensagem apresentada na Figura 4.5, porém estruturada de acordo com o padrão HL7 V3. O exemplo mostra o resultado do teste de glicose de um paciente, junto com informações adicionais que acrescentam semântica aos dados de forma hierárquica.

```
<observationEvent>
  <id root="2.16.840.1.113883.19.1122.4" extension="1045813"
     assigningAuthorityName="GHH LAB Filler Orders"/>
  <code code="1554-5" codeSystemName="LN"
       codeSystem="2.16.840.1.113883.6.1"
       displayName="GLUCOSE^POST 12H
CFST:MCNC:PT:SER/PLAS:QN"/>
  <statusCode code="completed"/>
  <effectiveTime value="200202150730"/>
  <priorityCode code="R"/>
  <confidentialityCode code="N"
    codeSystem="2.16.840.1.113883.5.25"/>
  <value xsi:type="PQ" value="182" unit="mg/dL"/>
  <interpretationCode code="H"/>
  <referenceRange>
    <interpretationRange>
       <value xsi:type="IVL_PQ">
       <low value="70" unit="mg/dL"/>
       <high value="105" unit="mg/dL"/>
      </value>
      <interpretationCode code="N"/>
    </interpretationRange>
  </referenceRange>
```

Figura 4.7. Exemplo de mensagem do resultado de um exame de glicose de um paciente no padrão HL7 V3. Em relação a conteúdo, os padrões HL7 V2 e V3 são igualmente abrangentes. Entretanto, no HL7 V3 a representação dos dados em XML facilita o entendimento do contexto. Contudo, aumenta-se o tamanho da mensagem em relação à versão anterior.

Além da padronização da representação de imagens, o **DICOM** especifica um protocolo para troca de mensagens. O protocolo fornece um arcabouço de comunicação para os serviços DICOM e é compatível com os protocolos TCP e IP. Essa compatibilidade possibilita a comunicação pela Internet entre aplicações distintas, que implementem o padrão DICOM. O protocolo de comunicação DICOM foi desenvolvido com base no mo-

[10]Disponível em https://www.ringholm.com/docs/04300_en.htm

delo de referência de Interconexão de Sistemas Abertos (*Open Systems Interconnection* – OSI) e implementa funcionalidades das camadas de aplicação, apresentação e sessão[11]. Uma aplicação que utiliza o protocolo DICOM é denominada Entidade de Aplicação (*Application Entity* – AE). Cada AE pode solicitar ou fornecer um dos serviços do protocolo DICOM e esses serviços são denominados classes de serviços. Cada classe de serviço consiste de dados e uma função relacionada àquele dado. Por exemplo, uma imagem de ressonância magnética pode ser associada a diferentes funções como imprimir ou armazenar. Quando uma AE solicita um serviço, desempenha o papel de Usuário de Classe de Serviço (*Service Class User* – SCU) e quando a AE fornece o serviço desempenha o papel de Provedor de Classe de Serviço (*Service Class Provider* – SCP). A comunicação entre duas AEs requer o estabelecimento de uma sessão, denominada "associação". O estabelecimento da associação inicia com a troca de informações importantes como a codificação de dados suportada e os serviços fornecidos pelo SCP. Após a associação, o SCU pode solicitar as classes de serviço ao SCP. Após o envio das classes de serviço, a associação é finalizada [Maani et al., 2011]. É importante destacar que, apesar de especificar um padrão de comunicação, o protocolo de comunicação DICOM não é genérico, sendo capaz de realizar apenas a troca de mensagens DICOM.

4.2.4. Padrões de terminologia

Os padrões de terminologias evitam a ambiguidade e aumentam a clareza do conteúdo ao armazenar informações em sistemas distintos, sendo essenciais para a interoperabilidade entre sistemas de registros médicos. Esses padrões definem um conjunto de códigos e sistemas de classificação que representam conceitos de saúde de forma a estabelecer uma forma de representação unificada [Massad et al., 2003].

No Brasil, a ANS em parceria com a AMB e o COPISS[12] desenvolveram a TUSS, que é um padrão de codificação de procedimentos médicos utilizados em planos de saúde privados. A tabela TUSS, como ficou conhecida, define a nomenclatura dos procedimentos médicos e seus respectivos códigos identificadores, grupos e subgrupos. Para facilitar a integração do padrão aos sistemas dos prestadores de serviços de saúde, a ANS disponibilizou o padrão TUSS como uma planilha como uma planilha em formato *xslx*[13]. Ao conceder a terminologia nesse formato, a TUSS possibilita que os usuários da planilha possam buscar códigos de procedimentos de forma ágil, utilizando o nome padronizado dos procedimentos e as ferramentas disponíveis em *software* de planilhas eletrônicas. Além disso, o formato em tabela agiliza a carga de novas atualizações do padrão para uma base de dados, permitindo que os sistemas integrados se mantenham atualizados.

O **SNOMED CT** [14] é um padrão de terminologia clínica multilínguas utilizado para representar conceitos médicos em sistemas de saúde, tendo como foco a integração de terminologias de vários países. O padrão tem uma grande abrangência, com mais de

[11] Disponível em https://docs.oracle.com/cd/E57425_01/121/IMDCM/ch_intro.htm#IMDCM13799

[12] Nota da ANS http://www.ans.gov.br/images/stories/Plano_de_saude_e_Operadoras/Area_do_consumidor/nota13_geas_ggras_dipro_17012013.pdf.

[13] Disponível em https://www.gov.br/ans/pt-br/arquivos/assuntos/consumidor/o-que-seu-plano-deve-cobrir/correlacaotuss-rol_2021_site.xlsx.

[14] Disponível em https://www.snomed.org/five-step-briefing.

350 mil conceitos médicos especificados em sua terminologia. Para organizar essa vasta coleção de conceitos, o padrão organiza os termos em três componentes:

- **Conceitos:** identificador único e computável, utilizado para garantir a unicidade de cada termo;
- **Descrições:** descrição de uma ideia clínica capturada de forma única e completa chamada de Nome Completamente Especificado (*Fully-Specified Name* – FSN), juntamente com um conjunto de sinônimos que guardam a informação do nome do termo nos múltiplos idiomas suportados pelo padrão;
- **Relacionamentos:** Registram as relações entre os conceitos, podendo ser de diversos tipos especificados pelo padrão. Relacionamentos podem representar hierarquia entre os conceitos, de forma que o conceito tem sempre no mínimo um relacionamento do tipo "é um", que define seu tipo.

Além de especificar a terminologia, o SNOMED CT especifica formas de implementação para o armazenamento dos dados de terminologia nos sistemas, servindo também como base para o auxílio no desenvolvimento de aplicações médicas. Um detalhe importante sobre o padrão é que, apesar de ser uma fundação sem fins lucrativos, a SNOMED cobra uma taxa para associação na organização e acesso à terminologia, caso o usuário venha de uma região sem órgãos federados à fundação[15].

Com o intuito de evitar ambiguidade nos campos de observação dos registros clínicos o **LOINC** propõe uma terminologia para os possíveis tipos de observação em resultados de exames e testes laboratoriais. Surgindo nesse contexto, o LOINC desenvolveu uma base de dados amplamente utilizada para categorização e identificação de observações de exames laboratoriais e dados clínicos, tais como observações clínicas, questionários e outras avaliações de saúde. O padrão define um conjunto de códigos numéricos e nomes padronizados para identificar as observações, aprimorando a comunicação e compartilhamento de dados entre sistemas de saúde. Em contraste com outras terminologias, o LOINC tem como objetivo principal criar diferentes códigos para cada tipo de teste, exame e observações, para serem usados nos campos de observação dos padrões de comunicação, como no HL7 v2. Paralelamente, o LOINC adiciona semântica às tradicionais terminologias difundidas, podendo combiná-las para expandir a capacidade de especificação e passagem de informação na troca de mensagem de registros médicos.

Para atingir seu o objetivo, o LOINC categoriza os códigos por meio de uma lógica de seis dimensões de especificação, sendo elas: (i) Componente (ou Analito), representando a substância ou entidade que está sendo medida ou observada; (ii) Propriedade, representando a característica ou atributo do analito; (iii) Tempo, representando o intervalo de tempo sobre o qual uma observação foi feita; (iv) Sistema, representando o espécime ou substância sobre a qual a observação foi feita; (v) Escala, definindo como o valor da observação é quantificado ou expresso; (vi) Método (opcional), representando uma classificação de alto nível de como a observação foi feita, geralmente utilizado quando a técnica afeta a interpretação clínica dos resultados.

[15]Disponível em `https://www.snomed.org/get-snomed`.

A união das seis dimensões da formalização do nome é chamada de FSN, que passa a ser, junto com o identificador numérico, a definição do tipo de observação. Além do FSN, o LOINC também especifica versões mais longas e humanamente legíveis do nome completo, o *Long Common Name* (LCN), juntamente com uma versão curta, o *Short Name*, para ser usada em colunas de tabelas ou relatórios. Apesar da especificação e definição de FSNs para as observação, apenas o código da especificação é enviado pelas mensagens. Para chegar na definição do código é necessário consultar a base do LOINC, utilizando o código numérico, através da API FHIR do LOINC[16], pela página *web* oficial ou tendo a base completa integrada ao sistema. A Tabela 4.2 apresenta um exemplo[17] dos passos para a especificação de uma observação para contagem manual de glóbulos brancos em amostra de líquido cefalorraquidiano. Esse processo mostra os passos que o LOINC segue para a categorização de forma única os diferentes tipos de observações clínicas, gerando, no fim, um identificador textual que resume completamente o contexto do valor da observação. O FSN, marcado em cinza claro e negrito, é formado pela junção das seis partes especificadas pelo padrão. As versões longas e curtas do nome também são apresentadas na tabela nas linhas em cinza claro.

Tabela 4.2. Exemplo da aplicação das seis partes do padrão LOINC para um exame de contagem manual de glóbulos brancos em amostra de líquido cefalorraquidiano, código LOINC 806-0. FSN marcado em cinza claro e negrito, formado pela junção das seis partes especificadas pelo padrão. Versões longas e curtas nas linhas em cinza claro.

Passo	Valor
Analito	Leukocytes
Propriedade	NCnc (*Number concentration*)
Tempo	Pt (*Point in time*)
Sistema	CSF (*Cerebral spinal fluid*)
Escala	Qn (*Quantitative*)
Método	*Manual Count*
FSN	**Leukocytes: NCnc: Pt: CSF: Qn: Manual count**
LCN	Leukocytes [#/volume] in Cerebral spinal fluid by Manual count
Short Name	WBC # CSF Manual

Com o intuito de aprimorar o levantamento estatístico das causas de morte e morbidade ao redor do mundo, a Organização Mundial da Saúde (OMS) desenvolveu o **ICD**, que atualmente está na 11ª edição, sendo referenciado como ICD-11. A classificação de doenças para registro com a finalidade de estudos estatísticos tem um papel fundamental na tomada de decisões em larga escala, com implicação no planejamento de ações governamentais e alocação de recursos de forma inteligente. Consequentemente, o impacto do planejamento baseado em dados leva a uma melhoria na qualidade dos serviços de saúde prestados à população [Harrison et al., 2021]. O ICD-11 é uma base de dados organizada de forma estatística e hierárquica que contém categorias para doenças e distúrbios, condições relacionadas à saúde, causas externas de doença ou morte, anatomia, ambientes, atividades, medicamentos, vacinas e outras informações que possam influenciar a saúde. Todos esses níveis de classificação são especificados na base de acordo com as

[16]Disponível em `https://loinc.org/fhir/`.

[17]Exemplo retirado da página *web* oficial do LOINC, disponível em `https://loinc.org/get-started/loinc-term-basics/`.

suas respectivas categorias, recebendo códigos de identificação alfanuméricos únicos e sequenciais, definindo uma hierarquia de doenças relacionadas [WHO, 2022].

Para consultas na base de dados do ICD-11 a OMS disponibiliza uma API REST sobre HTTP, interface gráfica *web*[18] e uma ferramenta de codificação, em que os usuários podem montar o código ICD-11 correto para uma doença e suas informações adicionais. A ferramenta é útil para teste e validação de *software* que utilize o sistema de códigos ICD-11. A Figura 4.8 apresenta a interface *web* da ferramenta de codificação do ICD, com destaque para um código ICD-11 gerado apenas selecionando as características de uma doença.

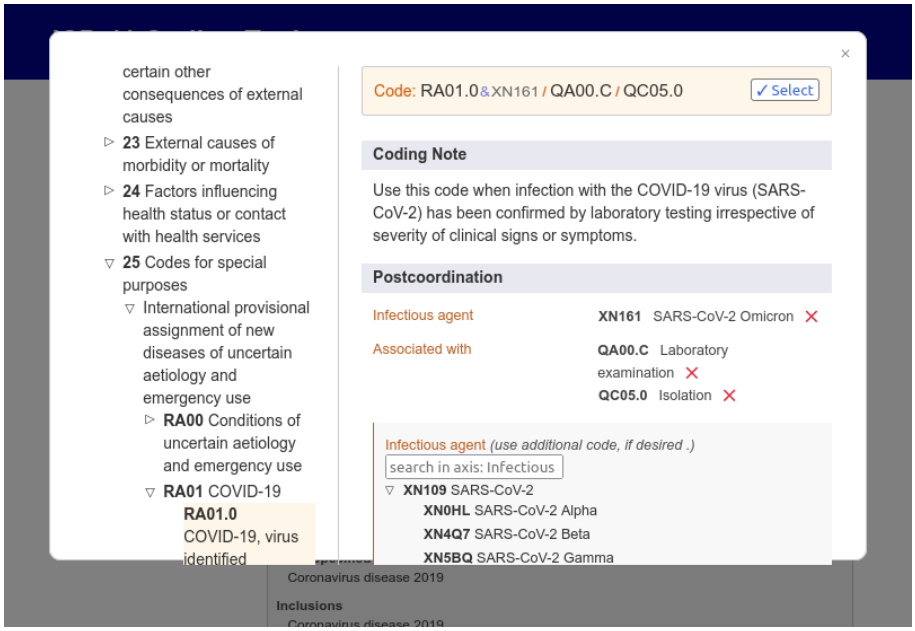

Figura 4.8. Aplicação *web* do ICD-11 disponibilizado pela OMS apresentando a ferramenta de codificação. O usuário pode buscar palavras-chave e selecionar a combinação de fatores desejada para um registro. O exemplo mostra o código gerado para a doença COVID-19 confirmada por teste laboratorial, com o vírus na sua variante SARS-CoV-2 Omicron, tendo o paciente em isolamento.

4.3. Fundamentos da Tecnologia de Cadeia de Blocos

A cadeia de blocos (*blockchain*) compreende uma tecnologia composta essencialmente por dois elementos básicos, uma estrutura de dados de encadeamento dos blocos e uma rede par-a-par (*Peer-to-Peer* – P2P) capaz de armazenar transações de forma ordenada e distribuída. Como principal diferencial, a tecnologia de cadeia de blocos viabiliza o desenvolvimento de aplicações distribuídas seguras em cenários marcados pela desconfiança mútua entre entidades, enquanto dispensa a necessidade de uma terceira entidade centralizadora, atuando como âncora de confiança para assegurar a segurança entre transações na rede [Mattos et al., 2018]. Diante dessas características, a cadeia de blocos é comumente interpretada como um livro-razão (*ledger*) distribuído por diversos terminais de uma rede.

[18]Disponível em `https://icd.who.int/browse11/l-m/en`.

Embora não haja unanimidade na literatura, as redes de cadeias de blocos podem assumir diferentes classificações: privada, pública, permissionada e não permissionada. Redes públicas e privadas contrapõem-se em relação ao controle de acesso à rede e ao conteúdo da cadeia. Redes públicas, de conteúdo aberto, são caracterizadas pela ausência de um mecanismo de controle de acesso. Além disso, a intermitência de nós em uma rede pública não causa quaisquer prejuízos ao mecanismo de consenso ou à geração de novos blocos. Diferentemente, as redes privadas detêm um conteúdo fechado e adotam medidas de controle de acesso restritas que impedem que nós sem autorização acessem a rede par-a-par e o conteúdo armazenado nos blocos da cadeia. As redes permissionadas e não permissionadas se diferenciam pelas atividades desempenhadas pelos nós na rede. Na rede não permissionada, há uma isonomia de papéis na rede, a qual garante que todos os nós possam desempenhar as mesmas funções, isto é, gerar transações, competir na mineração de blocos e participar do mecanismo de consenso. Em contraste, os nós pertencentes a redes permissionadas podem assumir papéis distintos de acordo com a necessidade da aplicação. Ao associar as características de cada par de classificações, cria-se a taxonomia de redes pública não permissionada, pública permissionada, privada não permissionada e privada permissionada [Mattos et al., 2018].

A tecnologia de cadeia de blocos oferece resistência à adulteração, uma vez que a alteração dos dados de um bloco de transações requer a manipulação de todos os blocos posteriores. Além disso, o caráter descentralizado das cadeias de blocos impede a existência de um ponto único de falha, centralizado, que prejudicaria a segurança e a privacidade das transações realizadas dado que eventuais conflitos de interesses entre as partes envolvidas podem ocorrer. Dessa forma, os nós participantes da rede par-a-par acessam uma réplica idêntica da cadeia de blocos armazenada localmente. Para evitar inconsistências e garantir a distribuição de réplicas coerentes dos dados, é necessário adotar mecanismos de validação e de consenso. Como os blocos da cadeia são compostos por uma sequência de transações a serem executadas, os nós precisam antecipadamente alcançar um consenso e concordar com as transações inseridas no bloco bem como com a ordem em que serão executadas. O processo de validação de transações, também denominado mineração, em certos casos, é desempenhado por um mecanismo de consenso. Esse mecanismo estabelece regras para validação e difusão de transações e blocos, resolvendo potenciais conflitos, e alcançando uma consistência eventual da informação presente na rede [Xu et al., 2017]. Ao se alcançar o consenso, garante-se a integridade, a consistência e a imutabilidade da cadeia de blocos. É válido destacar que cada bloco adicionado à cadeia tem como parte de seu conteúdo o resumo criptográfico do bloco anterior. Assim, os mecanismos de consenso e a forma como os blocos são encadeados tornam improvável a modificação do conteúdo de um bloco por um nó individual. Logo, há garantia de preservação do histórico de transações armazenadas nos blocos, impossibilitando a remoção ou edição de dados e a alteração da ordem das ações registradas. O registro de uma transação na cadeia de blocos requer que cada nó participante da rede aplique criptografia assimétrica, garantindo a veracidade e o não-repúdio dos dados armazenados. Também há garantia de pseudo-anonimato das partes envolvidas nas transações, uma vez que as identidades das partes são ocultadas da rede [Pustokhin et al., 2021].

Dentre os principais mecanismos de consenso para cadeias de blocos empregadas no setor de saúde estão:

- **Prova de Trabalho** (*Proof-of-Work* – PoW) é um mecanismo de consenso probabilístico que implementa uma lógica baseada na competição entre mineradores. Os mineradores são nós que buscam resolver um desafio criptográfico difícil para que as transações escolhidas sejam registradas em um bloco inserido na cadeia de blocos. A resolução do desafio é feita por força bruta e a solução é encontrada quando o nó descobre um valor numérico, chamado *nonce* criptográfico. Juntamente com as transações selecionadas, o *nonce* é adicionado ao bloco candidato a ser incorporado à cadeia de blocos. Em seguida, o bloco candidato é disseminado por toda a rede para que seja validado pelos demais nós. Para incentivar esse processo de resolução por força bruta, uma recompensa é oferecida ao minerador, ou grupo de mineradores, que primeiro resolver o desafio [Nakamoto, 2008]. Na PoW, a probabilidade de um nó conseguir minerar um bloco está atrelada ao poder computacional do nó.

- **Prova de Participação** (*Proof-of-Stake* – PoS) também é um mecanismo de consenso probabilístico, porém a probabilidade de sucesso na mineração de um bloco depende da participação dos nós na rede. Os nós mineradores competem para encontrar um valor de resumo criptográfico menor ou igual a um valor alvo para que possam minerar um bloco. Todavia, a dificuldade de determinar o resumo criptográfico é inversamente proporcional à riqueza acumulada (*coin age*) daquele nó. A riqueza acumulada é definida como a quantidade de recursos do nó multiplicada pelo período em que o nó reteve aquele recurso. Logo, o nó detentor da maior participação e riqueza acumulada, possivelmente terá a maior a probabilidade de validar o próximo bloco [Tschorsch e Scheuermann, 2016].

- **Prova de Autoridade** (*Proof-of-Authority* – PoA) é um mecanismo de consenso amplamente adotado em redes privadas caracterizado pela presença de uma entidade responsável por designar um conjunto de nós com autoridade. Os nós com autoridade são encarregados da tarefa de gerar novos blocos e validar as transações. Assim, a inclusão de qualquer bloco candidato na cadeia é precedida pela sua validação e assinatura por pelo menos um nó com autoridade. A manutenção da natureza distribuída da rede é garantida pela necessidade de uma concordância unânime entre os nós de autoridade sobre o estado global da cadeia. Para evitar disputas e desperdícios de recursos, algumas plataformas aplicam um esquema rotativo de geração de blocos, fato que garante um intervalo de tempo exclusivo a cada nó de autoridade. Eventuais falhas em nós de autoridade precisam ser detectadas pela plataforma e acarretam a remoção da autoridade do nó falho e a consequente desconsideração dos blocos minerados por ele [Cachin e Vukolic, 2017].

- **Raft** é o principal mecanismo de consenso usado no Hyperledger Fabric[19], recomendado para ambientes de produção [Carrara et al., 2020]. É um mecanismo tolerante a falhas de parada e é baseado no modelo líder-seguidor. O Raft alcança o consenso por meio da eleição de um líder, replicação de *log* e estágios de segurança. Os nós podem estar em três estados: candidato, seguidor ou líder. Inicialmente, os nós são seguidores e, se nenhum líder for detectado, ocorre uma eleição. O líder se comunica com os clientes, mantém o estado de seguidor e replica entradas de *log*.

[19]Disponível em `https://www.hyperledger.org/use/fabric`.

O líder usa uma chamada de procedimento remota *AppendEntries* para replicar *logs* e validar o estado do seguidor. O Raft garante que as transações sejam inseridas na mesma ordem nos nós e garante que o líder eleito tenha os *logs* mais recentes. O Raft oferece vantagens como fácil implementação em linguagens de programação mais comuns e um sistema de eleição eficiente. No entanto, requer capacidade de armazenamento significativa e tem limitações como a ausência de tratamento de falhas Bizantinas[20].

- **Tolerância Prática a Falhas Bizantinas** (*Practical Byzantine Fault Tolerance* – PBFT) é um mecanismo de consenso determinístico amplamente utilizado em sistemas distribuídos e plataformas de cadeia de blocos como Zilliqa e Hyperledger Fabric. O mecanismo lida com falhas no envio de mensagens e atrasos nas redes, assumindo falhas independentes e dependência parcial entre os nós. O PBFT garante segurança e vivacidade, mesmo com até $(n-1)/3$ nós maliciosos entre um total de n nós. O algoritmo envolve quatro etapas: (i) o cliente envia uma solicitação de transação ao líder; (ii) o líder a encaminha para outros nós; (iii) esses nós executam a requisição e (iv) enviam uma resposta ao cliente que espera $2f+1$ respostas consistentes, em que f é o número máximo tolerado de respostas falhas. O PBFT lida com líderes defeituosos por meio de troca de liderança baseada em alternância (*round-robin*). O mecanismo tem como vantagens o baixo consumo de energia e rápido tempo de execução em relação a outros mecanismos resistentes a falhas Bizantinas, mas apresenta limitações em redes maiores devido ao aumento da troca de mensagens e vulnerabilidade a ataques de personificação (*Sybil*). O PBFT é um mecanismo de consenso prático que garante comunicação e acordo confiáveis entre os nós, ao mesmo tempo em que mitiga o impacto de nós mal-intencionados [Carrara et al., 2020].

Introduzido primeiramente na plataforma de computação confiável Ethereum, o contrato inteligente (*smart contract*) consiste em uma aplicação autoexecutável armazenada na cadeia de blocos, que traduz as cláusulas de um contrato real para código. Através de um endereço conhecido e acessível, o contrato inteligente possui um conteúdo que pode ser inspecionado por todos os participantes da rede. Internamente, um contrato inteligente contém regras contratuais acordadas entre as partes, que tornam a violação proibitiva computacionalmente e, portanto, não vantajosa a potenciais violadores. Em contraste a contratos não determinísticos, que inviabilizam o consenso devido à aleatoriedade dos resultados atingidos por diferentes nós da rede, os contratos inteligentes são naturalmente determinísticos [Christidis e Devetsikiotis, 2016, Mattos et al., 2018], o que garante a convergência da visão global da rede. Como todas as interações com um contrato ocorrem via mensagens assinadas, é possível rastrear todos os participantes envolvidos na operação do contrato. O acionamento do contrato pode ser desencadeado por qualquer mudança de estado ou registro de transação na cadeia de blocos, facilitando a negociação, validação e execução comercial sem a necessidade de terceiros [Pustokhin et al., 2021]. Devido à imutabilidade da cadeia de blocos, quaisquer erros cometidos no código de um contrato inteligente já implementado não são passíveis de correção. Além disso, mudan-

[20]Falha Bizantina refere-se ao comportamento de um nó que foge ao comportamento esperado do protocolo definido.

ças nas circunstâncias relacionadas à execução do contrato, como modificações em leis e regulamentações, são igualmente complexas de serem contabilizadas pelo contrato já implementado. Isso impõe a necessidade de revisões extensas e potencialmente custosas do código do contrato inteligente por especialistas.

4.4. Desafios de Segurança e Privacidade no Acesso a Dados de Saúde

No Brasil, o aplicativo ConecteSUS[21] é responsável por disponibilizar informações de saúde do país. Na plataforma é possível que os cidadãos consigam, por meio de um dispositivo móvel ou acesso *web*, visualizar seu histórico clínico, incluindo carteira de vacinação, resultados de exames laboratoriais, medicamentos utilizados entre outras informações. Segundo o Banco Mundial, em 2022, o Brasil foi reconhecido como o segundo país do mundo com maior maturidade em governo digital[22]. Atualmente 80% da população brasileira, correspondendo a aproximadamente 140 milhões de usuários, já possui acesso a essas plataformas. Nos Estados Unidos, entre os anos de 2009 e 2019, houve mais de 3.000 violações de dados de saúde, cada uma envolvendo pelo menos 500 registros de pacientes. Em 2019, 572 violações envolvendo mais de 41 milhões de americanos foram relatadas [Luh e Yen, 2020]. Com o aprimoramento de modelos de inteligência artificial, os dados de pacientes podem ser utilizados para treinamento em servidores centralizados e com poucas camadas de segurança, facilitando a manipulação indevida dessas informações por atacantes [Rahman et al., 2021]. Esse treinamento sem as devidas regras de segurança, pode afetar hospitais que compartilham dados com entidades de pesquisa [Salim e Park, 2023], uma vez que são diretamente os responsáveis pela guarda desses dados.

Todos os ataques já conhecidos e amplamente explorados em sistemas computacionais, como Negação de Serviço Distribuído (*Distributed Denial of Service* – DDoS), *phishing*, *ransomware* e engenharia social, se aplicam também no contexto de registros médicos eletrônicos. A principal motivação dos atacantes está na comercialização de dados pessoais e, em alguns casos, espionagem relacionada ao roubo de patentes e propriedade industrial. Na maioria dos ataques bem sucedidos, a negligência e ingenuidade por parte dos usuários pode ser um fator decisivo para comprometer toda a infraestrutura e os sistemas, independente da finalidade. Ao utilizar senhas fracas, compartilhar credenciais e acessar sites e endereços *web* sem a devida atenção, o vazamento de dados pessoais pode acontecer de maneira quase que instantânea. Diante disso, criar mecanismos que garantam a transparência, confidencialidade e integridade dos registros médicos eletrônicos, torna-se indispensável no cenário atual. Tecnologias como cadeia de blocos e contratos inteligentes, podem e devem guiar os próximos anos de segurança computacional na área de saúde.

Uma das preocupações indispensáveis ao manipular EMRs é que esses dados são privados e pertencem aos pacientes, porém são totalmente controlados por instituições de saúde [Lesk, 2013]. Outra preocupação está relacionada ao Gerenciamento de Identidade (*Identity Management* – IM), pois aumenta a confiança e a privacidade dos sistemas de

[21] Disponível em https://conectesus.saude.gov.br/home.

[22] Disponível em https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2022/11/brasil-e-reconhecido-como-segundo-lider-em-governo-digital-no-mundo.

EMR [Tormo et al., 2013]. O IM para sistemas de armazenamento e consulta de registros médicos eletrônicos tende a ser centralizado, o que introduz um ponto único de falha e um gargalo de acesso para todo o sistema [Dubovitskaya et al., 2017]. Portanto, embora existam diferentes propostas baseadas em cadeia de blocos para armazenar e compartilhar os registros eletrônicos [Dubovitskaya et al., 2017, Zhang e Poslad, 2018, Yue et al., 2016], há oportunidade de melhoria para a oferta de um serviço mais seguro e adaptado às dores do mercado. Os sistemas EMR são comumente implementados com práticas precárias de segurança, podendo comprometer a privacidade e a confidencialidade dos dados do paciente [Jacquemard et al., 2020]. Além disso, o compartilhamento dos dados com finalidades comerciais pode ainda prejudicar a confiança nos planos e operadores de saúde. Os sistemas EMR possuem informações consideradas altamente confidenciais por vários motivos, havendo assim, uma forte necessidade de confidencialidade. A integridade dos registros médicos torna-se essencial, pois um tratamento incorreto baseado em dados errôneos pode ser fatal. Além disso, a disponibilidade é tão essencial quanto a integridade, pois as informações do sistema devem estar disponíveis para o tratamento adequado a qualquer instante [Haas et al., 2011]. O principal objetivo de um sistema EMR é a disponibilidade de dados do paciente. Nesse sentido, o controle de acesso não deve impedir qualquer solicitação legítima em nome do interesse vital dos pacientes [de Oliveira et al., 2023].

4.4.1. Controle de acesso a dados médicos

Um dos principais métodos para controle de acesso baseia-se na abordagem de permissionamento conhecida como Controle de Acesso baseado em Papéis (*Role-based Access Control* – RBAC). Nessa abordagem, cada usuário pode possuir um ou mais papéis, ou funções, tais como administradores, médicos, pacientes entre outros, definindo perfis distintos de permissão de acesso. Geralmente, um administrador fornece papéis específicos para cada usuário e cada função possui certos níveis de permissão. A Figura 4.9 apresenta o modelo de controle de acesso RBAC. Sistemas baseados nesse modelo podem comprometer a segurança pela complexidade no gerenciamento de grupos e usuários, em que permissões podem ser concedidas sem a real necessidade. No caso de registros médicos eletrônicos, o acesso aos dados do paciente tem como desafio determinar qual situação o paciente está em um dado momento. Uma consulta tradicional ou atendimento de emergência são exemplos dessas situações. No caso de emergência, o acesso aos dados deve ser permitido em caráter excepcional. O RBAC, por exemplo, não possui flexibilidade para acesso aos dados em casos imprevisíveis como em uma emergência. Nesse sentido, caso um paciente precise de atendimento e o médico disponível não tenha os papéis necessários naquele momento para acesso aos dados, o atendimento pode ser comprometido. Nesse sentido, alguns trabalhos propõem uma variação denominada Controle de Acesso baseado em Papéis de Emergência (*Emergency Role-Based Access Control* – E-RBAC), na qual são definidas as funções de emergência com base no nível de acesso que o usuário solicitante possui e posteriormente permite a consulta aos dados caso o paciente esteja na situação de emergência [Nazerian et al., 2019]. Embora diversas abordagens utilizem o RBAC como controle de acesso, esse modelo possui desafios quanto à escalabilidade, em função da possibilidade no aumento de papéis e políticas de forma indiscriminada [Seol et al., 2018].

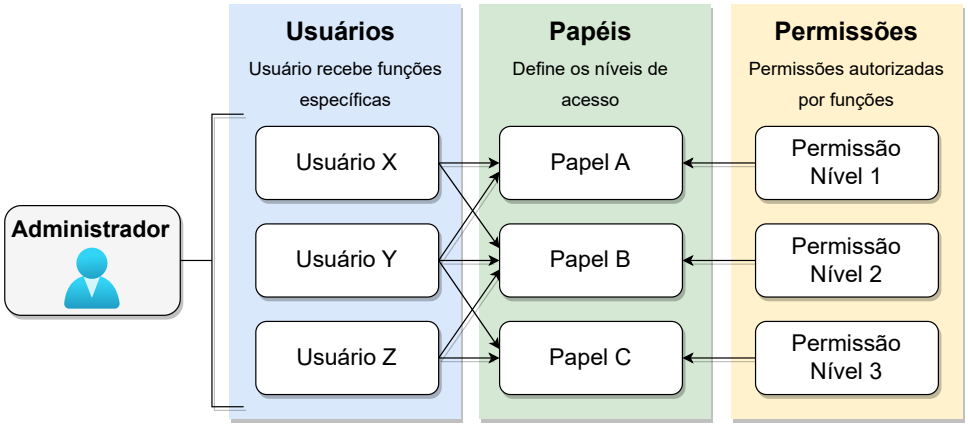

Figura 4.9. Modelo de controle de acesso baseado em papéis (RBAC). O administrador do sistema define quais os papéis e permissões existentes no sistema. Uma vez definidos, atribui para cada usuário um papel e o usuário pode exercer mais de um papel. Cada papel possui respectivos níveis de permissão.

Outra abordagem para controle de acesso é denominada SitBAC (*Situation-based access control*) [Peleg et al., 2008]. Essa abordagem considera a situação atual do paciente em vez do papel. A permissão de acesso aos dados é concedida mediante solicitações, diferentemente do RBAC que separa os usuários e suas permissões em relação a um conjunto de recursos. O SitBAC considera que a decisão da descoberta de dados dos pacientes é afetada por fatores que compõem a situação de acesso aos dados desses pacientes, como o solicitante dos dados, a tarefa a ser executada, uma autorização legal, entre outros. Cabe destacar que não fica evidenciado como o SitBAC pode ser utilizado juntamente com o RBAC, uma vez que ele é uma generalização ou superconjunto do RBAC. Além disso, o SitBAC não aborda questões básicas de segurança como confidencialidade, integridade e não-repúdio [Seol et al., 2018].

O modelo de Controle de Acesso baseado em Trabalho (*Work-based access control* – WBAC) foca o trabalho a ser executado pelo profissional e pela equipe. Nesse modelo, as atribuições de um dado usuário são modificadas de acordo com o tratamento que será desempenhado. Por exemplo, um cenário de separação de tarefas é utilizado para evitar fraudes através da identificação de papéis conflitantes [Abomhara e Ben Lazrag, 2016]. Nesse exemplo, um usuário em uma equipe só pode ser atribuído a um papel de equipe em um determinado momento. Nesse sentido, o modelo WBAC é definido pelos usuários atribuídos a papéis ou equipes, os membros da equipe que podem ser atribuídos a papéis de equipe e o trabalho, que pode ser atribuído a equipes. Por fim, as permissões podem ser associadas a papéis individuais e papéis de equipe [Abomhara et al., 2016]. Um dos principais desafios do WBAC é o gerenciamento das tarefas para cada usuário, o que pode aumentar a complexidade e erros durante atribuição dessas tarefas.

O modelo de Controle de Acesso baseado em Atributo (*Attribute-Based Access Control* – ABAC) define um paradigma de controle de acesso pelo qual os direitos de acesso são concedidos ao solicitante dos dados usando políticas que consistem em combinações lógicas de atributos. Os usuários devem estar cadastrados em um sistema central de IM, como Protocolo Leve de Acesso a Diretórios (*Lightweight Directory Access Pro-*

tocol – LDAP) ou Diretórios Ativos (*Active Directory* – AD), para que cada usuário seja associado a atributos já definidos no sistema. Esses atributos podem incluir atributos de usuário, de recursos e de ambiente, como ilustrado na Figura 4.10. Os atributos de usuário incluem informações como nome, cargo, função, organização, dentre outras. As informações relativas ao atributo de recurso podem conter data de criação, nome do recursos que pode ser acessado, dentre outras. O atributo de ambiente pode incluir informações geográficas do recurso a ser acessado. As políticas, solicitações e respostas ABAC são expressas na linguagem XACML. Uma política é uma combinação de regras que o solicitante deve obedecer. Quando uma solicitação é emitida, as regras expressas nas políticas são avaliadas, explorando os valores dos atributos para retornar uma resposta. As respostas contêm a decisão sobre o pedido. Em diversos casos, a operação dos sistemas de EMR possui um alto grau de complexidade. Em função disso, é possível haver negligências no controle de acesso, podendo ser mais permissivo do que o necessário, o que pode representar ameaças para as informações do paciente [de Oliveira et al., 2023]. Em alguns cenários, utiliza-se o modelo ABAC para obter uma maior granularidade no acesso às informações do paciente. No entanto, seu uso em cenários reais de saúde continua sendo um desafio, principalmente em casos nos quais o fluxo de trabalho durante cuidados intensivos, por exemplo, requer o compartilhamento de dados entre organizações, sendo difícil a sua modelagem. Consequentemente, os modelos de controle de acesso existentes utilizando ABAC geralmente cobrem apenas situações de acesso convencionais deixando os cuidados intensivos sem a devida proteção de acesso [de Oliveira et al., 2023].

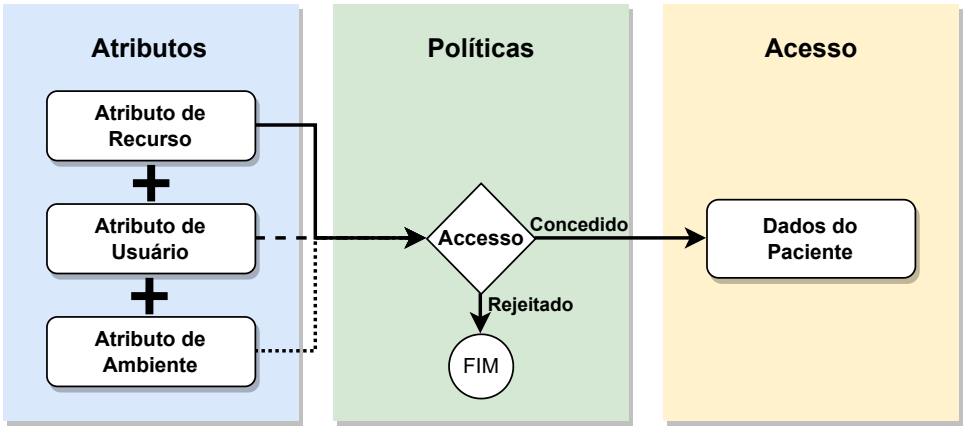

Figura 4.10. Modelo de controle de acesso baseado em atributos (ABAC). Existem basicamente três tipos de atributos, os de Recurso, os de Usuários e os de Ambiente. Os atributos associados a cada usuário diferenciam a permissão de acesso desses usuários. A combinação dos atributos executa uma política de permissão ou rejeição ao acesso.

Outra abordagem é o Controle de Acesso baseado em Propósito (*Purpose-based access control* – PBAC), que tem como objetivo relacionar os dados com finalidades específicas. Esse mecanismo aproveita as características do ABAC e RBAC, sendo capaz de utilizar tanto papéis como atributos. A ideia central desse modelo é conceder acesso mediante o entendimento prévio em que um dado pode ser coletado ou acessado. Os propósitos são organizados de forma hierárquica, através de princípios de generalização e especialização [Byun et al., 2005]. Esse fato pode contribuir significativamente para a

privacidade de dados sensíveis, embora o gerenciamento possa induzir uma maior complexidade em função do controle de cada propósito.

O padrão XACML define cinco componentes principais que lidam com decisões de acesso: *Policy Administration Point* (PAP), *Policy Enforcement Point* (PEP), *Policy Decision Point* (PDP), *Policy Information Point* (PIP) e *Context Handler* (CH). O PAP armazena e gerencia um conjunto persistente de políticas associadas aos identificadores de destino. O PEP constitui a integração para qualquer sistema, em que os recursos a serem protegidos são armazenados e gerenciados. O PEP recebe as solicitações de acesso e bloqueia o fluxo de execução até que uma decisão seja tomada. Ao mesmo tempo, o PEP propaga as solicitações para o PDP, que é o principal local de decisão para a solicitação de acesso recebida. O PDP recupera todos os atributos necessários e informações contextuais do PIP, avalia as políticas definidas e toma uma decisão de acordo com essas políticas. O PIP é responsável por recuperar e armazenar valores de atributos. O Context Handler (CH) é responsável por derivar o contexto de uma determinada solicitação. A Figura 4.11 exibe as diversas interações entre os componentes do padrão XACML, destacando a sequência cronológica das trocas de mensagens durante o processo de requisição de acesso. Antes de uma solicitação de acesso, é necessário que (1) o PAP escreva políticas e conjuntos de políticas e os torne disponíveis ao PDP. O solicitante do acesso (2) envia uma solicitação de acesso ao PEP, podendo incluir valores de atributos dos assuntos, recursos e ambiente. Os atributos de assuntos dizem respeito ao paciente na condição de emergência. Em seguida, (3) o PEP constrói um Contexto de requisição XACML padrão e o envia para o PDP, que (4) solicita quaisquer valores adicionais de atributo de assunto, de recurso e de ambiente do PIP. O PIP obtém os atributos solicitados e (5) os devolve ao PDP. Por sua vez, o PDP (6) solicita ao PAP as políticas de acordo com o objetivo do pedido. O PAP (7) retorna as políticas de solicitação para que o PDP (8) avalie a política relacionada e retorne o Contexto de Resposta XACML padrão para o PEP. Por fim, o PEP (9) executa a decisão de autorização, seja ela permitindo ou negando o acesso.

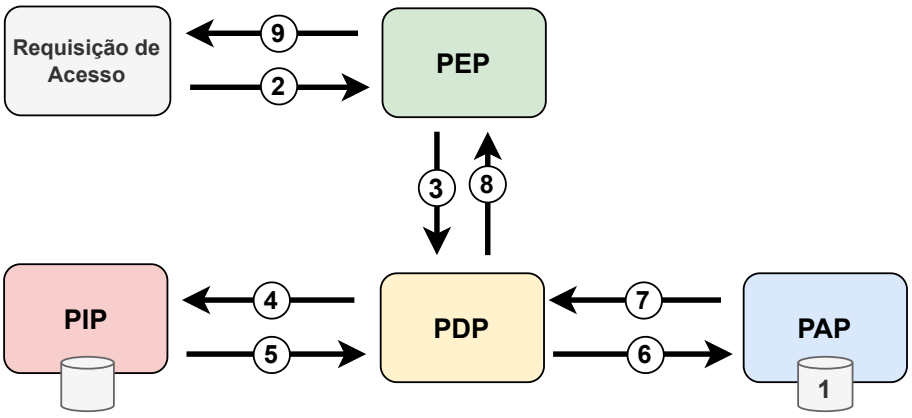

Figura 4.11. Arquitetura e fluxograma do padrão XACML. As interações entre os componentes do padrão XACML ocorrem em ordem cronológica, devendo haver uma definição de políticas para que a consulta possa ser realizada resultando em permissão ou negação de acesso aos dados solicitados.

4.4.2. Normas e legislações para proteção de dados

Políticas de proteção de dados privados, cada vez mais severas, impõem limites para abordagens centralizadas de processamento de dados. As leis de proteção de dados pessoais estipulam direitos aos titulares dos dados e obrigações às instituições que detêm tais dados. Uma lei de destaque é o Regulamento Geral de Proteção de Dados (*General Data Protection Regulation* – GDPR)[23], vigente em toda a União Europeia (UE), que estabelece diretrizes quanto ao tratamento, por uma pessoa, empresa ou organização, dos dados pessoais de todos na União Europeia. Para cumprimento da lei, é essencial realizar previamente o processo de identificação de dados sensíveis. Isso envolve diversas etapas para garantir que os dados pessoais nos armazenamentos de dados da organização sejam tratados adequadamente. A etapa inicial é descobrir e localizar dados pessoais nos repositórios de dados da organização. Uma vez identificados, os dados são categorizados com base em sua natureza e sensibilidade. Posteriormente, são implementadas medidas adequadas para proteger os dados sensíveis identificados.

Cada categoria de dados confidenciais pode ter requisitos de privacidade específicos, como criptografia, tempo de custódia, segurança física e lógica. A GDPR define categorias especiais, como dados raciais e de saúde. Ao lidar com essas categorias, uma empresa deve ter uma base válida e legal para coletar, armazenar, transmitir ou processar os dados. Além disso, podem ser aplicadas salvaguardas e considerações mais rígidas para garantir a privacidade e a segurança dessas categorias especiais de dados [Larrucea et al., 2020]. Um dos principais desafios no tratamento de registros médicos eletrônicos é o fato de a GDPR enfatizar a necessidade de consentimento por parte dos paciente para manipulação dos dados. Os requisitos fundamentais para eficácia desse consentimento são definidos no artigo 7º da GDPR, o qual especifica que quando o processamento for baseado no consentimento, o controlador dos dados deve ser capaz de demonstrar que o titular dos dados consentiu o tratamento de seus dados pessoais. Além disso, ao avaliar que tal consentimento é fornecido de maneira espontânea, a execução de um contrato, incluindo a prestação de um serviço, está condicionada ao consentimento para o processamento de dados pessoais que não são necessários para a execução daquele contrato. Tradicionalmente, os contratos e consentimentos são efetuados através de documentos impressos ou digitais. Esses documentos possuem complexidade desde a geração, manipulação e armazenamento, tanto do ponto de vista logístico quanto de segurança. Nesse sentido, abordagens utilizando contratos inteligentes distribuídos podem ser considerados fundamentais na transição para um mundo completamente digital.

No caso do Brasil, a Lei Geral de Proteção de Dados (LGPD) promulgada em 2018, é uma lei federal responsável pela proteção de dados em todo território nacional. Similar à GDPR, a LGPD se aplica a qualquer organização que processe dados pessoais no Brasil, independentemente de estar sediada ou não em território nacional. A lei define dados pessoais de forma ampla, como qualquer informação relacionada a uma pessoa natural ou pessoa jurídica de direito público ou privado. Entende-se por informações pessoais nome, endereço, e-mail, número de telefone, número de identificação, endereço IP, entre outras. A lei identifica como agentes de tratamento a pessoa natural ou jurídica de direito público ou privado que realiza qualquer operação de tratamento sobre os dados

[23]Disponível em `https://gdpr-info.eu/`.

pessoais de outrem. Dentre os deveres estabelecidos a esses agentes estão a coleta de consentimento explícito do titular do dado e a disponibilização de relatórios que identifiquem as operações de tratamento aplicadas ao dado, incluindo a especificação de seu local de armazenamento, mascaramento do dado e medidas de proteção. Diversas organizações devem implementar medidas técnicas e organizacionais para garantir a segurança e confidencialidade dos dados pessoais, devendo relatar quaisquer violações de dados à Autoridade Nacional de Proteção de Dados (ANPD) e aos indivíduos afetados. A ANPD é responsável por policiar o cumprimento da LGPD, impondo multas e penalidade.

Pela LGPD, os dados de saúde são considerados dados pessoais sensíveis e seu processamento está sujeito a regras específicas. Assim como a GDPR, o tratamento dos dados sensíveis exige o consentimento por parte do titular ou seu responsável legal, de forma específica e destacada, para finalidades específicas[24]. Outro documento comumente utilizado é o Termo de Consentimento Livre e Esclarecido (TCLE). Esse documento é assinado pelo paciente ou seu responsável legal, com o objetivo de esclarecer dúvidas acerca das possíveis intercorrências, riscos envolvidos ou outras informações pertinentes a um determinado tratamento ou procedimento médico. Por possuir informações sensíveis, os dados presentes nesse documento também são regidos pela LGPD. Na maioria dos casos, esse termo é preenchido e assinado manualmente, o que pode dificultar o sigilo das informações nele contidas. Embora haja uma migração cada vez maior para a digitalização desses dados, existem diversos problemas a serem resolvidos. Um dos principais desafios encontrados no Brasil referente ao acesso aos dados digitalizados, é a carência de acesso à Internet em áreas periféricas das grandes cidades e também em áreas rurais. Esse fato implica diretamente os pacientes, uma vez que sem acesso à Internet ficariam impedidos de acessar seus registros médicos. Outro desafio, é o fato de não haver no Brasil, legislação específica para tratamento de registros médicos eletrônicos, diferentemente dos Estados Unidos que possui a Lei de Portabilidade e Responsabilidade de Seguro Saúde (*Health Insurance Portability and Accountability Act* – HIPPA).

Diferentemente da GDPR e LGDP, que são leis gerais para dados pessoais, a HIPAA é uma legislação dos Estados Unidos, promulgada em 1996, criada especificamente para proteção das informações de saúde dos indivíduos. Ela estabelece padrões de privacidade e segurança para as informações médicas, conhecidas como informações de saúde protegidas (*Protected Health Information* – PHI) e restringe o acesso e a divulgação desses dados por parte dos profissionais de saúde, provedores de serviços médicos e empresas de seguros. Existem ainda, diretrizes de privacidade para definir os termos relacionados aos direitos e os limites de privacidade dos pacientes, para que possam compreender e controlar seus dados [Lee et al., 2021]. Essas diretrizes utilizam sete termos principais:

- **Compreensão dos pacientes:** Os pacientes possuem o direito de compreender os procedimentos para armazenar, utilizar e reter suas informações de saúde pelos profissionais de saúde;
- **Confidencialidade:** Os dados de saúde são protegidos durante o armazenamento e transmissão utilizando técnicas como criptografia, autenticação. Sob nenhuma

[24]Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

circunstância os dados de saúde do paciente devem ser divulgados a terceiros sem prévia autorização;

- **Controle dos pacientes:** Os pacientes devem ter a capacidade de controlar e autorizar quem pode acessar e utilizar seus dados de saúde;
- **Integridade dos dados:** As informações eletrônicas de saúde dos pacientes devem ser protegidas contra modificações ou destruição não autorizadas;
- **Exceção de consentimento:** Em situações excepcionais em que um paciente corre risco de vida ou em outras circunstâncias críticas, as informações de saúde podem ser divulgadas e usadas sem a autorização individual do paciente;
- **Não-repúdio:** Para garantir que as autoridades responsáveis cumpram suas obrigações em relação às informações dos pacientes, quaisquer atividades relevantes devem ser apoiadas por evidências verificáveis;
- **Auditoria:** O monitoramento regular das informações de saúde dos pacientes e o registro abrangente das atividades relacionadas são necessários para garantir a segurança dos dados. Os pacientes devem receber garantias quanto à segurança e proteção de suas informações de saúde.

A ideia central do tratamento de privacidade da HIPPA é garantir que as informações de saúde dos indivíduos sejam devidamente protegidas, permitindo o fluxo de informações de saúde necessárias para fornecer e promover cuidados de saúde. A HIPAA estabelece um equilíbrio que permite a utilização de informações importantes, ao mesmo tempo em que protege a privacidade das pessoas que buscam atendimento. Existe um vasto mercado de saúde nos Estados Unidos, amplamente diversificado e a regulamentação HIPAA é projetada para que seja flexível e abrangente, permitindo cobrir uma variedade de usos e divulgações que precisam ser abordadas[25]. Outro aspecto importante da HIPAA é a maneira que aborda casos de violações de informações de saúde. Segundo a regulamentação, uma violação geralmente ocorre através do uso ou divulgação não autorizada sob a "Regra de Privacidade" que compromete a segurança ou a privacidade das informações de saúde protegidas. A "Regra de Privacidade" estipula padrões para proteção dos registros médicos dos indivíduos e outras informações de saúde, passíveis de identificação individual. Essa regra exige a guarda adequada das informações de modo a garantir a privacidade de dados protegidos, além de garantir o direito de examinar e obter uma cópia de seus registros de saúde. Pressupõe-se que o uso ou a divulgação não autorizados de informações de saúde protegidas seja uma violação, a menos que a entidade coberta (planos de saúde, hospitais e clínicas) ou parceiro comercial demonstre que há uma baixa probabilidade de que as informações de saúde confidenciais tenham sido comprometidas com base em uma avaliação de risco. Há ainda três exceções no que diz respeito à definição de violação. A primeira exceção se aplica à aquisição, acesso ou uso não intencional de informações de saúde protegidas por um membro da força de trabalho ou pessoa agindo sob a autoridade de uma entidade coberta ou parceiro comercial, se tal

[25]Disponível em https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

aquisição, acesso ou uso foi feito de boa fé e dentro o alcance da autoridade. A segunda exceção se aplica à divulgação inadvertida de informações de saúde protegidas por uma pessoa autorizada a acessar tais informações em uma entidade ou parceiro comercial coberto para outra pessoa autorizada a acessar essas informações na entidade ou parceiro comercial ou organização de assistência médica. Em ambos os casos, as informações não podem ser usadas ou divulgadas sem a devida autorização mediada pela "Regra de Privacidade". A terceira exceção se aplica à entidade coberta ou ao parceiro comercial acreditar de boa fé que a pessoa não autorizada, a quem a divulgação sem autorização foi feita, não seria capaz de reter as informações[26].

4.5. Soluções para Integração e Compartilhamento Seguro de Dados de Saúde

A integração e o compartilhamento seguro de dados de saúde são temas fundamentais para a evolução dos sistemas de saúde. O avanço da tecnologia e a digitalização dos registros médicos originam diversos desafios relacionados à interoperabilidade e à proteção da privacidade dos pacientes. Os dados dos pacientes estão pulverizados em diversos silos de dados que não se comunicam e não utilizam necessariamente o mesmo padrão de representação e comunicação, o que dificulta a troca de informações de forma eficiente e segura. Mesmo que seja possível a troca de informação, o compartilhamento de informações sensíveis requer medidas robustas de proteção, como criptografia e controle de acesso, para garantir que apenas pessoas autorizadas tenham acesso aos dados e que a integridade desses dados seja preservada. Assim, a falta de padronização, a diversidade de sistemas, a segurança dos dados e questões regulatórias tornam a integração e o compartilhamento seguro um aspecto complexo na área de saúde. Diversas soluções têm sido desenvolvidas para enfrentar essas questões, visando melhorar a qualidade do atendimento, facilitar a troca de informações entre profissionais e garantir a segurança dos dados sensíveis. Nesse contexto, exploram-se algumas das soluções disponíveis no mercado e propostas na literatura para promover a integração e o compartilhamento seguro de dados de saúde.

4.5.1. Abordagens Tradicionais

Tradicionalmente, a segurança dos dados nos estabelecimentos de saúde é garantida por meio do uso de sistemas de acesso restrito, protegidos por *firewalls*, com normas rígidas relativas à amplitude e quantidade de dados de paciente que podem ser arquivados. Mais recentemente, protocolos de criptografia foram aplicados.

O sistema eletrônico **e-SUS Atenção Primária (APS)**[27] reúne diversas ferramentas voltadas para a reformulação da Atenção Básica (AB) a fim de informatizar o Sistema Único de Saúde (SUS). Atualmente, o e-SUS é composto por dois sistemas de *software* complementares, capazes de instrumentalizar o processo de coleta de dados médicos. O Prontuário Eletrônico do Cidadão (PEC) foca o armazenamento de todas as informações clínicas e administrativas do paciente, no contexto da Unidade Básica de Saúde (UBS),

[26]Disponível em https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

[27]Disponível em https://sisaps.saude.gov.br/esus/.

isto é, qualquer estabelecimento de saúde enquadrado como posto de saúde, centro de saúde básica, unidades mistas ou centro de apoio à saúde da família. O *software* de Coleta de Dados Simplificada (CDS) dedica-se exclusivamente a estruturar a digitação do cadastro e das fichas de atendimento, sendo especialmente adaptado para cenários sem informatização ou com conectividade limitada, instável ou inexistente. Para tal, a inserção de dados no CDS pode ser realizada de maneira *off-line* e posteriormente consolidada através de um PEC com conectividade. A simplicidade do CDS acarreta uma limitação na capacidade de armazenamento local no banco de dados embarcado, além de inviabilizar funções gerenciais.

Independentemente do *software* de coleta utilizado, os dados são encaminhados ao Sistema de Informação em Saúde para a Atenção Básica (SISAB), responsável pela centralização nacional do processamento e pela disseminação de dados e informações relacionadas à AB. Antes de serem disponibilizados no sistema, os dados enviados são submetidos a um processo de validação a fim de verificar a originalidade, o cumprimento de critérios temporais e o vínculo com um estabelecimento registrado no Cadastro Nacional de Estabelecimentos de Saúde (CNES). Com base nos dados consolidados, o SISAB emite relatórios de desempenho contendo indicadores de saúde por estado, município, região de saúde e equipe. O controle de acesso aos recursos dentro do e-SUS é baseado em perfis de acesso, ou papéis, em que cada perfil é associado a um conjunto de recursos do sistema que podem estar ativos ou inativos, dependendo das atividades desenvolvidas pelo profissional. A integração com sistemas terceirizados é viabilizada através da API do *Apache Thrift* ou adotando arquivos padronizados no formato XML. Dessa forma, o sistema já existente em uma unidade de saúde deve ser capaz de gerar arquivos Thrift/XML, que são importados para o PEC municipal. O PEC é capaz de gerar relatórios de inconsistências e controlar a transmissão dos dados para o SISAB por meio de um sistema centralizador nacional. Ambas as alternativas, Thrift ou XML, garantem a interoperabilidade do e-SUS APS com sistemas já implementados em municípios, permitindo a importação dos dados coletados e a consolidação no SISAB.

A plataforma **AGHUx** (Aplicativo de Gestão para Hospitais Universitários)[28] tem como foco a gestão de hospitais universitários e auxilia a padronização das práticas assistenciais e administrativas desses hospitais. O sistema é desenvolvido pela Empresa Brasileira de Serviços Hospitalares (EBSERH) e prevê o acesso unificado a todos os registros eletrônicos de saúde gerados pelos hospitais integrantes da rede. Essa integração proporciona uma visão transversal sobre a trajetória clínica do paciente, aprimorando a continuidade de tratamentos e atendimentos independente do hospital de origem. O acesso remoto às informações médicas registradas no AGHUx é viabilizada através do HU Digital[29], uma plataforma digital disponível tanto no formato *web* quanto por meio de aplicativos em dispositivos móveis. O HU Digital oferece interfaces distintas dependendo se o perfil de usuário que o acessa é um profissional de saúde ou um paciente. Os pacientes têm acesso aos próprios históricos de dados, além de usufruir de serviços digitais, como emissão de certificados e realização de teleconsultas. Atualmente, a permissão de acesso pode ser concedida a pessoas físicas ou a hospitais universitários específicos

[28]Disponível em https://www.gov.br/ebserh/pt-br/hospitais-universitarios/regiao-centro-oeste/hujm-ufmt/governanca/aghu.

[29]Disponível em https://hudigital.ebserh.gov.br/.

da rede. Analogamente, médicos e enfermeiros devidamente autorizados podem se autenticar no HU Digital a fim de consultar sumários de alta, procedimentos e cirurgias realizadas ou agendadas.

A Figura 4.12 destaca os módulos que compõem o AGHUx. Os módulos são dedicados a funções administrativas e a procedimentos médicos. O módulo Pacientes lida com o cadastramento dos pacientes no sistema, subsidiando as demais atividades de atendimento. Dependendo do procedimento realizado no hospital, pode-se realizar a abertura de prontuário. Através do módulo Prontuário *On-Line* (POL) são visualizadas todas as informações clínicas do paciente, contemplando seu histórico de registros de atendimentos realizados. O módulo Ambulatório Administrativo é acionado em situações que exijam procedimentos simples como realização de curativos, pequenas cirurgias, primeiros socorros. O módulo Ambulatório Assistencial permite ao médico analisar a evolução do atendimento dentro do consultório. O módulo Internação apoia a gestão das internações hospitalares, com funcionalidades de admissão, gestão de leitos, atribuição dos profissionais responsáveis, emissão de sumário de alta e realização de alta médica e administrativa. O módulo Prescrição de Enfermagem auxilia na definição dos cuidados aplicados a cada paciente, com base nos dados coletados e analisados e do diagnóstico estabelecido pela equipe de enfermagem. O módulo Controle de Paciente visa informatizar os registros dos controles do paciente, abrangendo os processos de monitorizações e controle hídrico, permitindo agilidade na visualização da informação e maior segurança na assistência ao paciente. O módulo Prescrição Médica registra os diagnósticos e as prescrições médicas, gerando condutas e atividades para a equipe assistencial. O módulo Exames consolida os registros de Serviços de Apoio ao Diagnóstico e Terapêutico (SADT) em um conjunto organizado de elementos, incluindo solicitações, acompanhamento e resultados. O módulo Farmácia compreende o processo de gestão dos medicamentos, incluindo atividades de regulação, triagem e dispensação. Intimamente atrelado ao anterior, o módulo Estoque concentra-se em gerenciar as movimentações dos suprimentos através do controle do fluxo de materiais, proporcionando um eficaz atendimento das solicitações de materiais. O módulo Cirurgia detalha quaisquer ações relacionadas a procedimentos cirúrgicos complexos, tais como descrição do procedimento, agendamento de sala, medição do tempo de utilização e cálculo de custos. Devido à modularidade do sistema, o principal desafio enfrentado pelo AGHUx é o descompasso entre as versões do sistema implantadas nos hospitais universitários e a implantação dos módulos, que podem não ser compatíveis com a versão do sistema existente no hospital.

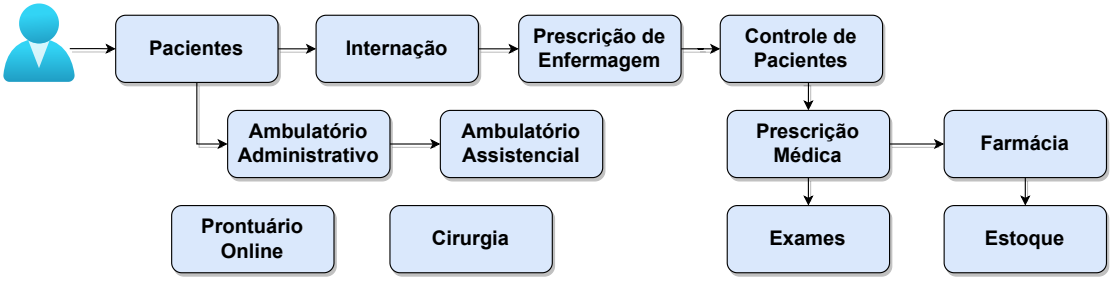

Figura 4.12. Visão geral dos módulos integrantes do sistema AGHUx e interação entre esses módulos.

Algumas soluções disponíveis comercialmente têm como foco áreas específicas da saúde, como o **iDoc**[30], criado para radiologia odontológica. O iDoc é uma plataforma para distribuição *online* de exames e diagnósticos, que reúne dados e exames dos pacientes enviados por diferentes clínicas radiológicas. Assim, o iDoc centraliza as informações dos pacientes, permitindo que o dentista tenha acesso aos dados dos pacientes mesmo que os exames tenham sido realizados em clínicas diferentes. O dentista pode também adicionar informações sobre o paciente, incluindo o histórico e a anamnese. A plataforma dispensa o uso de exames impressos, permitindo o compartilhamento *online* dos exames digitais, que são armazenados em nuvem. O iDoc tem capacidade de hospedar arquivos digitais em formatos como JPEG, DICOM, STL, PLY, PPTZ, DOCX e PDF[31]. A plataforma tem como vantagem a rapidez e a agilidade com que o exame fica disponível para consulta. Assim que o exame é finalizado, a clínica pode enviá-lo ao dentista. A plataforma também oferece uma variedade de recursos, como uma ferramenta de modelo digital que permite analisar a arcada dentária do paciente em formato tridimensional. Não há informações disponíveis sobre como o controle de acesso aos dados é realizado.

Outro sistema comercial é o **Alert**[32], adaptado para *web* e nuvem. O Alert é destinado ao gerenciamento completo do processo clínico eletrônico por meio de diversos produtos que compõem a solução. Inclui diversas funcionalidades para o acompanhamento do histórico de cada paciente, agendamento e alertas de consultas ou procedimentos médicos, atribuição de altas, emissão de relatórios, teleatendimento e gestão de pedidos. Além disso, o *software* dispõe de um sistema interno de planejamento e de inteligência empresarial. A solução utiliza padrões de interoperabilidade e suporte IHE, HL7 e ITIL, e terminologias internacionais, como SNOMED, ICD, LOINC, dentre outras. O acesso aos diversos produtos é feito por meio de um mecanismo *Single Sign-On* (SSO) que fornece aos usuários um esquema de autenticação centralizada em todo o domínio das aplicações Alert. O SSO suporta a integração dos produtos Alert com domínios LDAP ou AD. O acesso aos dados dos pacientes é feito com base em perfis pré-definidos associados a cada profissional cadastrado no sistema.

O **GestãoDS** é um *software* médico com agendamento *online*, controle financeiro, telemedicina, *marketing* médico e outras funcionalidades criadas para facilitar a gestão de clínicas e consultórios. O *software* também oferece assinatura digital e garante privacidade dos dados no processamento, na manutenção e no armazenamento de informações relacionadas à saúde em conformidade com a HIPAA. A solução fornece vários níveis de permissão de acesso, separados em perfis de usuários. Além disso, oferece modelos personalizados de prontuários e prescrições de acordo com o padrão de atendimento do profissional.

4.5.2. Abordagens baseadas em cadeia de blocos

A incorporação da tecnologia de cadeia de blocos em diversas aplicações tem sido amplamente motivada pela possibilidade de gerar evidências computacionais irrefutáveis, armazenadas de forma distribuída, da ordem cronológica das transações realizadas. Esses benefícios são desejáveis em soluções de compartilhamento de EMRs, visto que há

[30]Disponível em https://idoc.radiomemory.com.br/.
[31]Disponível em https://blog.radiomemory.com.br/conheca-o-idoc-academico/.
[32]Disponível em https://www.alert-online.com/br/.

necessidade de rastreabilidades dos dados acessados. Nesse sentido, diversas soluções baseadas em cadeia de blocos são propostas na literatura, sendo algumas delas disponibilizadas comercialmente. Dentro do âmbito comercial, a plataforma **Medicalchain**[33] constitui-se como um mercado de dados de saúde acessado por MedTokens. Quinhentos milhões de MedTokens foram emitidos e vendidos em 2018. Nessa solução, o paciente controla o acesso dos médicos aos registros, por exemplo, durante uma consulta de telemedicina, e podem conceder a pesquisadores acesso aos registros em troca de MedTokens. Os MedTokens também podem ser usados para pagar consultas médicas [Albeyatt, 2018]. A solução é construída com base em duas cadeias de blocos e não armazena dados médicos nos blocos. A primeira é usada para controlar o acesso aos EMRs e é implementada utilizando a plataforma Hyperledger Fabric. A segunda cadeia é usada para geração dos *tokens*, o que é feito por meio do Pedido de Comentários Ethereum 20 (*Ethereum Request for Comments 20* – ERC20)[34] da Ethereum. A distribuição do *token* é controlada por um contrato inteligente. Assim, a Ethereum é usada para pagamentos. Semelhante à Medicalchain, a solução **MedChain** usa dois tipos de *tokens* distintos: *tokens* externos, denominados MedCoins, para fornecer controle de acesso e privacidade; e *tokens* internos, denominados *Record Tokens*, para fornecer um mapa do registro do paciente distribuído, adicionando resumos criptográficos à cadeia de blocos [Sandgaard e Wishstar, 2018]. A plataforma de cadeia de blocos utilizada é a Ethereum para ancoragem de verificação e a Hyperledger Fabric. Os registros na MedChain podem incluir dados de saúde em vários formatos, como texto simples, imagens digitais ou objetos de banco de dados. Essas informações são armazenadas em um sistema de arquivos distribuído com base no Sistema de Arquivos Interplanetário (*InterPlanetary File System* – IPFS). O endereço do registro de um paciente armazenado no sistema de arquivos é associado ao "bloco de paciente" daquele paciente na Ethereum. Para recuperar todos os registros do paciente, há interação com um contrato inteligente para obtenção de todos os endereços de todos os registros do paciente. Ao obter os endereços, é possível utilizá-los para solicitar cada registro ao IPFS. Outras soluções como a **MediBChain**, fornecem privacidade [Al Omar et al., 2017] e protegem a identidade do paciente utilizando o pseudonimato através de chaves públicas criptográficas. A proposta implementa um sistema de gerenciamento de dados de saúde centrado no paciente baseado em cadeia de blocos permissionada. Não há informação sobre a plataforma utilizada.

Dentre as soluções acadêmicas, a proposta **AuditChain** fornece controle de acesso multinível para pacientes, médicos, enfermeiros e administradores hospitalares para o gerenciamento de EMRs [Anderson, 2018]. A proposta implementa contratos inteligentes utilizando a plataforma Hyperledger Fabric [Rebello et al., 2019, Agrawal et al., 2022]. A assinatura digital da transação usa criptografia de chave pública e serve como um *token* virtual para controle de acesso. A proposta **Medblock** [Fan et al., 2018] implementa uma estrutura de compartilhamento de dados com um mecanismo de controle de acesso baseado em um esquema de assinatura. Os dados confidenciais e os ponteiros para o EMR do paciente são criptografados com um esquema de assinatura múltipla dentro da cadeia de blocos. O mecanismo de controle de acesso percorre os blocos até encontrar o bloco correto comparando a assinatura com a coleção de assinaturas no livro-razão. A permissão

[33] Disponível em `https://medicalchain.com/en/`.

[34] Padrão de *Fungible Token* que implementa uma API para *tokens* em contratos inteligentes.

para ver o conteúdo criptografado no bloco depende do resultado da comparação. Zhang *et al.* propõem o **FHIRChain** para compartilhamento de dados entre médicos e pesquisadores com base no padrão FHIR [Zhang et al., 2018]. O FHIRChain atende a cinco requisitos principais de interoperabilidade: identificação e autenticação do usuário, troca segura de dados, acesso autorizado a dados, formatos de dados consistentes e modularidade do sistema. O controle de acesso aos dados é baseado em um contrato inteligente que resulta em um *token* de acesso e executa na plataforma Ethereum. Os *tokens* de acesso são definidos para cada transação de dados, que usa criptografia assimétrica para proteger os ponteiros de dados fora da cadeia. A proposta usa as identidades digitais de saúde dos usuários para criptografar o conteúdo, de modo que apenas os usuários que possuem as chaves privadas de identidade digital corretas possam descriptografar o conteúdo. Dagher *et al.* propõem a **Ancile**, uma cadeia de blocos baseada em Ethereum para um sistema de gerenciamento de registros que utiliza contratos inteligentes para maior controle de acesso e ofuscação de dados [Dagher et al., 2018]. A Ancile mantém os registros médicos dos pacientes nos bancos de dados existentes dos provedores e os endereços de referência a esses registros e suas permissões para cada registro são armazenados no contrato inteligente. A Ancile foi projetada para armazenar os endereços Ethereum de todos os nós que podem interagir com um registro, um nível de acesso e uma chave simétrica criptografada com a chave pública de cada nó. Em contrapartida, Oliveira *et al.* desenvolvem uma abordagem de distribuição de EMR cujo controle de acesso é centrado no paciente [de Oliveira et al., 2019]. A abordagem depende de uma infraestrutura de chave pública (*Public Key Infrastructure* – PKI) e da tecnologia cadeia de blocos. A ideia é herdar a confiança na autenticidade fornecida pela PKI e a integridade e a responsabilização fornecidas pela cadeia de blocos. A proposta é um EMR distribuído, com infraestrutura computacionalmente simples, controle de acesso refinado e baixa sobrecarga.

Rouhani *et al.* propõem um sistema ABAC para compartilhamento de dados EMR [Rouhani et al., 2021], ao passo que Maesa *et al.* propõem um sistema ABAC usando a plataforma de cadeia de blocos Ethereum [Maesa et al., 2019]. Ao optarem pelo armazenamento dos valores dos atributos na cadeia de blocos, os valores não podem ser alterados devido à propriedade de imutabilidade. Em compensação, os valores são auditáveis, visto que suas atualizações podem ser executadas apenas por meio de transações e assim registradas na cadeia de blocos. Não obstante, ambas as propostas não consideram que os atributos devam ser autenticados pelas organizações do processador do dado sempre que interagem com o sistema de controle de acesso. Por ser um sistema assíncrono, a cadeia de blocos exige que as organizações atualizem continuamente os atributos de seus profissionais na cadeia de blocos, fato que onera atributos dinâmicos dos profissionais de saúde. Por outro lado, Ghorbel *et al.* propõem manter os atributos do usuário fora da cadeia de blocos (*off-chain*) e confiar nas autoridades confiáveis para manter uma lista de usuários associados aos seus atributos verificados [Ghorbel et al., 2021]. Empregando um contrato inteligente, essas autoridades autenticam os atributos do usuário durante a solicitação de dados do usuário. Os autores utilizam a plataforma Quorum, que implementa uma versão permissionada da cadeia de blocos Ethereum. Internamente, a plataforma Quorum adota um mecanismo de consenso flexível, capaz de suportar o consenso RAFT para tolerância a falhas de travamento e variações do PBFT para tolerância a falhas bizantinas.

Ao associar a tecnologia de cadeia de blocos e um esquema de assinatura baseado em atributos sobre múltiplas autoridades, Guo *et al.* propõem um sistema de EMR distribuído [Guo et al., 2018] que permite ao paciente gerenciar com segurança Registros Pessoais de Saúde (*Personal Health Record* - PHR). No entanto, essa facilidade também traz um custo de desempenho, pois cria uma sobrecarga para assinar a transação por várias autoridades. A proposta também sofre de questões de confidencialidade relativas aos dados armazenados na cadeia de blocos. De maneira semelhante, Dang *et al.* analisam o uso da computação em névoa para armazenar e proteger EMRs e usam assinaturas baseadas em atributos para garantir privacidade e confidencialidade de EMR em ambientes de névoa e nuvem [Dang et al., 2018]. Por sua vez, Yue *et al.* concentram-se em fornecer um controle de privacidade refinado [Yue et al., 2016]. O sistema proposto usa telefones celulares para interagir com um *gateway* de controle de acesso que controla o acesso aos blocos na cadeia de blocos. No entanto, o *gateway* não controla as transações. Daraghmi *et al.* propõem um mecanismo de consenso baseado em incentivo que alavanca o grau de reputação dos provedores de saúde em relação aos seus esforços na manutenção de registros médicos e na criação de novos blocos na cadeia de blocos [Daraghmi et al., 2019]. O contrato de controle de acesso inclui todas as informações relacionadas às permissões específicas para cada registro baseado em contratos inteligentes. A proposta lista os endereços da cadeia de blocos Ethereum para todos os usuários que têm permissões de acesso ao registro. O contrato especifica o nível de acesso e a chave simétrica criptografada com a chave pública de cada usuário.

No Brasil, existe uma solução governamental notória para compartilhamento de dados de saúde em rede nacional, a **RNDS**[35] (Rede Nacional de Dados em Saúde). A RNDS é uma plataforma de integração desenvolvida pelo DataSUS e pela Secretaria Executiva do Ministério da Saúde. Quando integralmente consolidada, a RDNS pretende incluir um repositório de informações retrospectivas, simultâneas e prospectivas do paciente em formato digital. Sua utilização permitirá que inúmeros estabelecimentos compartilhem informações transversais de atendimento do cidadão de forma integrada, contínua, eficiente e de qualidade. Para simplificar a interoperabilidade dos prontuários do cidadão, a RNDS prevê que o histórico de registros médicos do paciente seja disponibilizado em uma estrutura de cadeia de blocos compartilhada entre os estados. A arquitetura da plataforma é apresentada na Figura 4.5.2. A plataforma conta com uma infraestrutura hospedada em nuvem com contêineres dedicados e distribuídos para os estados federados. Cada contêiner é subdividido em serviços informacionais e serviços tecnológicos, classificados tanto de acordo com o tipo, por exemplo, conjunto mínimo de dados ou relacionados à segurança, quanto conforme o grau de maturidade de desenvolvimento do serviço, como disponíveis ou planejados [Santos et al., 2022].

Os serviços tecnológicos disponíveis incluem o **Master Pacient Index** (MPI), um banco de dados que atua unificando as informações de cada paciente registrado por uma organização de saúde. Sendo um padrão de projeto de *software*, o **Backend For Frontend** (BFF) é responsável pela entrega de como as informações serão armazenadas e consultadas, independentemente das especificidades de cada tipo de interface gráfica, por exemplo, aplicativo e portal *web*. Os **Serviços Eletrônicos de Saúde** (*EHR-Service*)

[35] Disponível em `https://www.gov.br/saude/pt-br/assuntos/rnds`.

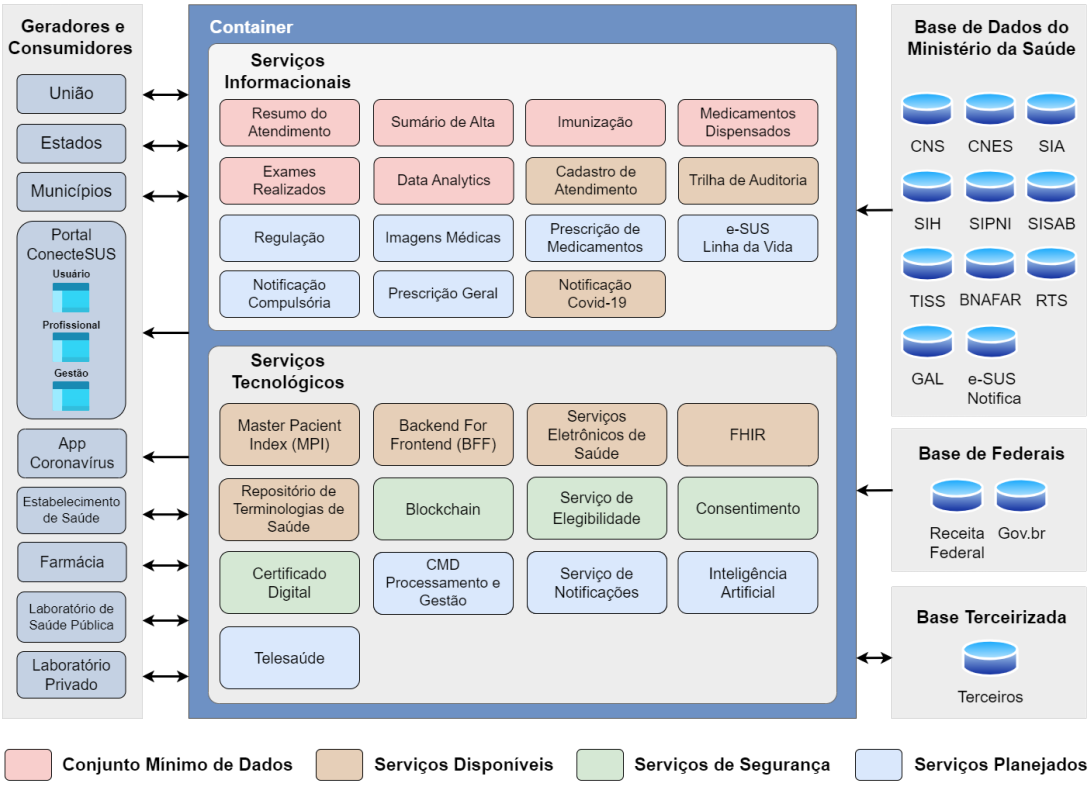

Figura 4.13. A RNDS é uma solução governamental para integração de sistemas de saúde e compartilhamento de dados de saúde em território nacional. A plataforma ainda está em desenvolvimento e conta com diversos módulos ainda não implementados.

concentram os serviços RESTful na troca de informações entre as aplicações de Saúde Digital, em especial o PEC, portais e aplicações *web*. O padrão **FHIR** auxilia na troca de informações de saúde entre diferentes estabelecimentos e instituições. O **Repositório de Terminologias em Saúde** é um ambiente virtual nacional que abriga classificações, nomenclaturas, terminologias, taxonomias, modelos de informação e definições comuns necessárias para a padronização de recursos semânticos e modelos de informação a serem utilizados no setor de saúde [Santos et al., 2022].

Dentre os serviços tecnológicos de segurança, o mais relevante é o relacionado à tecnologia de cadeia de blocos. A RNDS prevê a implementação de uma cadeia de blocos privada e permissionada, baseada em Hyperledger Fabric, e executando o mecanismo de consenso Raft [Tribunal de Contas da União (TCU), 2020]. Cada contêiner representa um nó de cadeia de blocos e estará localizado em um estabelecimento de saúde. A adoção da cadeia de blocos visa o armazenamento do histórico de interações entre pacientes e profissionais de saúde além de conter referências para os registros de saúde eletrônicos. Atualmente, a cadeia de blocos da RNDS possui apenas um nó, o que não garante as propriedades características da tecnologia. O processo de recuperação dos dados de saúde de qualquer paciente via cadeia de blocos, precisa satisfazer algumas premissas: (i) a requisição de acesso deve ser originada de uma ferramenta de *software* apropriada; e (ii) o solicitante deve integrar um estabelecimento cadastrado no CNES e deve possuir credenciais corretas. Caso um profissional requisite o acesso a qualquer documento ou

registro médico do paciente, somente é atendido mediante o consentimento e autorização explícita do paciente, ou em circunstâncias médicas emergenciais, ou quando configurada a estratégia "*opt out*" no contexto de atendimento no estabelecimento de saúde. A estratégia "*opt out*" assume de antemão que o paciente autoriza a flexibilização das regras de acesso aos seus dados. Assim, caso deseje alterar a política de permissão, o paciente poderá fazê-lo mediante à solicitação [Tribunal de Contas da União (TCU), 2020]. Internamente, os metadados são utilizados no livro-razão e distribuídos entre os diversos participantes da rede. Os documentos clínicos serão utilizados em uma coleção de dados privados (*private data collection*), um recurso nativo da Hyperledger Fabric, que permite que um subconjunto definido de organizações consiga endossar, confirmar ou consultar dados privados sem a necessidade de criar um canal separado. Esse recurso garante a privacidade e economicidade de armazenamento do documento. Uma vez que os documentos serão armazenados apenas na organização custodiante e em uma estrutura limitada de organizações de *backup*, não haverá eventual armazenamento excessivo dos documentos clínicos. Como é compartilhado no livro-razão, o histórico do paciente estará acessível para qualquer organização, o que facilitará as consultas dos pacientes nos estabelecimentos de saúde. A interoperabilidade entre sistemas é assegurada pela adoção do padrão FHIR e terminologia LOINC para o tráfego e armazenamento dos dados. Inicialmente, a RNDS prevê a utilização de microsserviços de transição, capazes de realizar a conversão dos dados enviados em CDA, OpenEHR e FHIR. Para evitar o preenchimento incompleto ou impressos de registos médicos, a plataforma pretende implementar contratos inteligentes escritos na linguagem GO, assegurando que as regras de negócio envolvidas nos registros do prontuário eletrônico sejam efetivamente cumpridas [Tribunal de Contas da União (TCU), 2020].

A RNDS complementa a segurança agregada ao sistema pela cadeia de blocos oferecendo serviços como: (i) emissão de **Certificados Digitais**, isto é, documentos eletrônicos contendo dados sobre a pessoa física ou jurídica que o utiliza, servindo como uma identidade virtual que confere validade jurídica e aspectos de segurança digital; (ii) **Serviço de Elegibilidade**, serviço validador dos dados disponibilizados que define se o profissional de saúde está habilitado ou não a acessar os dados do cidadão, aplicando regras de vinculação do profissional com o estabelecimento de saúde, CPF, categoria profissional, certificação da instalação de prontuário eletrônico; (iii) **Consentimento**, relacionado ao modelo de consentimento *opt-out*. Por padrão, assume-se a existência de um consentimento implícito, até que o cidadão opte pela revogação explícita do consentimento [Santos et al., 2022].

Avaliações preliminares utilizando a prova de conceito arquitetural estimam que a RNDS poderá suportar até 1.800 transações por segundo (tps), taxa satisfatória para suportar a quantidade anual de atendimentos prevista no SUS [Tribunal de Contas da União (TCU), 2020]. Atualmente, o Ministério de Saúde disponibiliza três portais[36] de acesso às informações armazenadas na RNDS, o ConecteSUS Cidadão, ConecteSUS Profissional e ConecteSUS Gestão, direcionados aos pacientes, aos profissionais de saúde e aos gestores, respectivamente. Ao acessar o portal, cidadãos obtêm o histórico vacinal e outros registros pessoais de saúde, profissionais de saúde visualizam toda a trajetória clínica e

[36]Disponível em `https://conectesus.saude.gov.br/home`.

de procedimentos dos seus pacientes e gestores conseguem acompanhar a evolução dos indicadores de saúde, fundamentais para coordenação de políticas públicas. A Tabela 4.3 sintetiza as principais características apresentadas por soluções de saúde baseadas em cadeias de blocos.

Tabela 4.3. Características relacionadas às soluções de saúde baseadas em cadeias de blocos.

Tipo	Características	**MediBChain** [Al Omar et al., 2017]	**MedicalChain** [Albeyatt, 2018]	**MedChain** [Sandgaard e Wishstar, 2018]	**Patel** *et al.* [Patel, 2019]	**Ghorbel** *et al.* [Ghorbel et al., 2021]	**AuditChain** [Anderson, 2018]	**FHIRChain** [Zhang et al., 2018]	**MedRec** [Azaria et al., 2016]	**Medblock** [Fan et al., 2018]	**Ancile** [Dagher et al., 2018]	**RNDS**[37]
Cadeia de Blocos	Privada Permissionada										✓	✓
	Pública Permissionada	✓				✓		✓		✓		
	Privada Não Permissionada				✓							
	Não Especificado		✓[1]	✓[1]			✓[1]		✓[1]			
Mecanismo de Consenso	Prova de Trabalho	✓						✓	✓		✓	
	Prova de Participação				✓							
	Consenso Raft											✓
	Tolerância Prática a Falhas Bizantinas		✓	✓								
	Consenso Híbrido ou Próprio									✓		
	Não Especificado					✓[2]	✓[2]					

✓[1]: Os autores apenas informam que a cadeia de blocos é permissionada, não a especificando-a como pública ou privada. Contudo, assume-se como uma rede privada.
✓[2]: Os autores apenas informam que o mecanismo de consenso adotado é flexível.

4.6. Discussão, Tendências e Desafios de Pesquisa

Embora seja potencialmente utilizável, a tecnologia de cadeia de blocos ainda é considerada um tecnologia complementar aos sistemas legados e não os substitui. A Tabela 4.5 resume os principais obstáculos técnicos na incorporação da tecnologia de cadeia de blocos no setor de saúde. A **escalabilidade** apresenta-se como um potencial entrave à adoção convencional de cadeias de blocos nos setores de saúde. Embora não seja impactante em cadeias de blocos privadas, a falta de escalabilidade é claramente uma questão preocupante em cadeias de blocos públicas. Comparada às redes de transações tradicionais, capazes de processar milhares de transações por segundo, as cadeias de blocos públicas limitam-se a dezenas de transações por segundo [Chowdhury et al., 2019, Lo et al., 2017]. Dependendo da plataforma e do mecanismo de consenso implementado, a latência introduzida pelo processo de validação de um bloco pode alcançar até 10 minutos [Chowdhury et al., 2019]. Ademais, a escolha inadequada do mecanismo de

[37]Disponível em https://www.gov.br/saude/pt-br/assuntos/rnds.

Tabela 4.4. Vantagens e desvantagens apresentadas por diferentes soluções acadêmicas de EMR baseadas em cadeias de blocos.

	Diferencial	Vantagens	Desvantagens
[Dubovitskaya et al., 2017]	Sistema EMR baseado em cadeia de blocos permissionada	Privacidade dos dados de usuário	Controle de acesso limitado aos dados de pacientes
[Azaria et al., 2016]	Sistema EMR baseado em cadeia de blocos pública	Controle de acesso baseado em contratos inteligentes	Alto processamento computacional
[Guo et al., 2018]	Sistema EMR distribuído	Assinaturas baseadas em atributos para gerenciamento de PHR	Custos de sinalização e problemas de confiabilidade
[Dang et al., 2018]	Sistema EMR baseado em nuvem e névoa	Assinaturas baseadas em atributos para confidencialidade e privacidade	Custos de sinalização e ambiente limitado
[Yue et al., 2016]	Sistema EMR baseado em *gateway*	Controle de privacidade grosseiro	Controle limitado de transações
[Makary e Daniel, 2016]	Mercado de dados de saúde	Controle de privacidade centrado no paciente	Gerenciamento complexo do MedToken
[Al Omar et al., 2017]	EMR centrado no paciente	Pseudoanonimato de chaves públicas	Gerenciamento complexo de chaves
[Anderson, 2018]	Controle de acesso em multinível	Token vitual para assinatura digital de transação	*Scripts* de solicitação complexos
[Uddin et al., 2018]	Agente centrado no paciente	Controle de acesso baseado em papéis	Alto custo de processamento
[Zhang e Poslad, 2018]	Controle de acesso em camadas	Controle de permissão refinado	Longos atrasos de validação e recuperação
[Xia et al., 2017]	Sistema com controle e gerenciamento de dados baseado em cadeia de blocos	Controle de acesso complexo	Chave de acesso e escalabilidade
[Liang et al., 2017]	Sistema móvel de compartilhamento de registro médico baseado em cadeia de blocos	Compartilhamento de dados colaborativo e uso de árvore com raiz de Merkle para segurança	Interoperabilidade
[Jiang et al., 2018]	Sistema para intercâmbio de dados baseado em cadeia de blocos	Integra abordagens fora da cadeia e a verificação na cadeia para garantia de privacidade e autenticidade	Complexidade do sistema de acesso e desempenho
[Fan et al., 2018]	Sistema de compartilhamento eficiente e seguro baseado em cadeia de blocos	Gerenciamento e compartilhamento de registros de sistemas de EMR e mecanismo de acesso	Suscetibilidade a falhas devido ao alto custo de processamento

consenso impacta no aumento do tempo de criação de blocos. Paralelamente, à medida que o número de transações e nós na rede aumenta, mais verificações devem ser realizadas e, consequentemente, maior a probabilidade de formação de gargalos. Sob a ótica de sistemas de saúde, esses potenciais atrasos afetam adversamente a análise de exames e a definição rápida de diagnósticos [De Aguiar et al., 2020]. Contudo, há uma pluralidade de abordagens capazes de resolver essa questão. Uma das abordagens é a utilização de *sharding*, uma técnica baseada na divisão da rede em diferentes fragmentos (*shards*), de modo que a duplicação compulsória da comunicação, do armazenamento de dados e da sobrecarga de computação seja evitada para cada nó participante. Essa abordagem desobriga que cada nó lide com toda carga transacional da rede, permitindo que apenas mantenham os dados sobre seu fragmento [Yu et al., 2020]. Outra abordagem consiste em modificar a tradicional estrutura linear das cadeias de bloco para uma representação na forma de Grafo Acíclico Direcionado (*Directed Acyclic Graph* – DAG). Nessa nova estruturação, cada transação é vinculada a múltiplas transações, permitindo o paralelismo do processo de validação [Kaur e Gandhi, 2020].

Os sistemas de saúde baseados em cadeias de blocos são desenvolvidos agrupando conceitos multidisciplinares que englobam tanto conhecimentos de tecnologia da informação quanto competências e fluxos de atendimento da área médica. Contudo, a baixa presença de profissionais qualificados e a alta complexidade de manipulação e manutenção contribuem para tais sistemas serem frequentemente vinculados à fraca **usabilidade** [De Aguiar et al., 2020]. Em 2019, o Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) apontou que apenas 20% dos estabelecimentos de saúde, sejam eles privados ou públicos, detinham um profissional com formação na área da saúde alocado em seus respectivos departamentos de TI. Essa escassez de profissionais de saúde atuantes na área técnica é igualmente acompanhada na porcentagem de presença de equipes de TI internas em estabelecimentos de saúde. No cenário brasileiro, por exemplo, 21% dos estabelecimentos de saúde têm uma equipe interna destinada ao suporte técnico na área de TI, enquanto 39% deles tinham um prestador de serviço contratado pelo próprio estabelecimentos [Cetic.br, 2020]. As dificuldades são reduzidas ao priorizar a criação de interfaces intuitivas e habilitadas para os usuário.

Intrínseca às cadeias de bloco, a característica de imutabilidade estabelece que após registrados nos blocos, os dados armazenados não são passíveis de alteração. Como cada nó da rede detém uma réplica da cadeia, qualquer tentativa de modificação dos dados em uma dessas réplicas é traduzida pelos nós participantes como um ataque iminente. Como consequência, essas tentativas de alteração são rejeitadas, impossibilitando o apagamento ou edição dos dados, que não pode ser feito nem mesmo pelos próprio autores ou por ordem judicial [Mattos et al., 2018]. Essa característica impõe aos sistemas baseados em cadeia de blocos a necessidade de lidar com a **irreversibilidade** dos registros realizados na cadeia. Embora a autenticidade seja inviolável numa cadeia de blocos, não há garantias sobre a precisão dos dados armazenados. Assim, blocos contendo informações falsas ou incorretas, mesmo que intencionalmente inseridas, não podem ser removidos ou modificados. A inflexibilidade na manipulação dos dados contrasta-se com necessidades de armazenamento presentes em sistemas de EMR. Por não apresentarem atributos críticos ou valiosos para diagnósticos futuros, alguns dados são armazenados temporariamente. Outros dados como endereço ou características pessoais dos pacientes, embora não sejam críticos, requerem atualizações constantes. Ambas as situações destacam que o armazenamento indiscriminado de dados na cadeia de blocos é um fator limitante para a adoção da tecnologia, dada a impossibilidade de exclusão de registros antigos. Outro fator desafiador é a exposição de chaves privadas. Caso ocorra, os dados dos pacientes estarão expostos para quaisquer indivíduos ou entidades detentores da chave privada, não havendo a possibilidade de utilizar uma nova chave para criptografar novamente os dados já registrados na cadeia. Portanto, qualquer vazamento de chave expõe permanentemente a privacidade do paciente caso seus dados sejam gravados na cadeia [Lo et al., 2017].

Outro aspecto sensível remete à **privacidade e segurança** dos dados, visto que todos os nós acessam os dados transmitidos por outro nó. Ao acessar suas próprias informações ou histórico médico, os pacientes são dependentes de uma entidade intermediadora, caso ocorra uma emergência. Esse fator rompe os princípios de privacidade estabelecidos nas legislações vigentes de proteção de dados. A expansão do poder computacional dos sistemas modernos representa sérias ameaças à segurança da cadeia de blocos, sobretudo quando se baseiam em criptografia de chave pública. Tal vulnerabilidade relaciona-se

à suposição de que os computadores clássicos são incapazes de fatorar grandes números rapidamente. Contudo, essa hipótese é refutada perante o surgimento da computação quântica, uma tecnologia emergente que pretende resolver desafios criptográficos altamente complexos de maneira rápida e eficiente. Dentre as alternativas para enfrentamento desse desafio, ressalta-se a substituição das assinaturas digitais convencionais por criptografia resistente a *quantum* [Yaqoob et al., 2022]. Paralelamente, redes baseadas em PoW também são propensas a violar a segurança criptográfica. Essa violação ocorre através do Ataque de 51%, uma ação maliciosa em que um grupo de mineradores detém a fração majoritária do poder computacional da rede de cadeia de blocos e, portanto, esses nós ditam o processo de adição de blocos à rede [Mattos et al., 2018]. Logo, um sistema de saúde prejudicado por esse ataque pode significar a perda de credibilidade das organizações.

Para usufruir do potencial da tecnologia de cadeias de blocos em cuidados de saúde, é essencial abordar os desafios relacionados à **interoperabilidade**. Essa propriedade remete à capacidade de trocar informações entre sistemas com características heterogêneas. Para tornar dois sistemas de EMR interoperáveis, as mensagens de transmissão devem ser baseadas em dados codificados padronizados. Embora a ausência de padrões de cadeias de blocos simplifique a função dos desenvolvedores, essa indefinição contribui para problemas de comunicação entre sistemas distintos. Assim, a falta de interoperabilidade entre sistemas é potencializada pela existência de várias redes de cadeias de blocos baseadas em diferentes mecanismos de consenso, mecanismos de transação e funcionalidades de contratos inteligentes. No âmbito de saúde, a adoção de tecnologias clínicas, especificações técnicas e capacidades funcionais tradicionalmente díspares, também trava a criação e compartilhamento de dados em um formato único. Constata-se que, mesmo desenvolvidos sobre a mesma plataforma, diversos sistemas de EMR não são interoperáveis dado que foram projetados para atender necessidades e preferências específicas de uma instituição de saúde. Na prática, a falta de dados padronizados limita a capacidade de compartilhar os dados eletronicamente para o atendimento ao paciente. Uma solução plausível para esse problema é o desenvolvimento de novos padrões, que possam ser aderidos por soluções legadas. Com esse propósito, a *Enterprise Ethereum Alliance*[38] (EEA) introduziu uma versão padronizada da cadeia de blocos Ethereum [Yaqoob et al., 2022, Mattos et al., 2018].

Além dos desafios técnicos relacionados à adoção da cadeia de blocos, também existem diversos desafios relacionados aos sistemas de saúde. Destacam-se desafios de interoperabilidade entre sistemas, padronização e integração dos dados, segurança dos dados e privacidade. A **interoperabilidade entre os sistemas** é particularmente importante para permitir o acesso rápido e fácil a informações precisas e atualizadas sobre os pacientes para tomar decisões clínicas bem informadas. Contudo, tanto o gerenciamento de dados de saúde quanto a interoperabilidade entre os sistemas são desafiadores devido à heterogeneidade de informações e sistemas. Os diversos sistemas devem ser desenvolvidos levando em consideração as boas práticas da segurança da informação. Os dados de saúde devem ser padronizados para permitir a consistência e a interoperabilidade entre sistemas distintos. Os padrões também regem a captura, armazenamento e recuperação da informação. Dessa forma, os sistemas desenvolvidos devem estar em conformidade com os

[38]Disponívem em `https://entethalliance.org/`.

Tabela 4.5. Desafios enfrentados no emprego da tecnologia de cadeia de blocos em sistemas de saúde.

Obstáculo Técnico	Desafios
Escalabilidade	Tamanho do bloco e tempo de criação do bloco
	Adoção de mecanismos de consenso ineficientes
	Tempos de confirmação mais altos para a criação de um bloco
	Aumento exponencial do número de verificações conforme cresce o número de transações e nós na rede
Usabilidade	Complexidade no desenvolvimento e manutenção de sistemas de saúde baseados em cadeia de blocos
	Carência de profissionais familiarizados com a gestão de redes par-a-par complexas
Irreversibilidade	Imutabilidade das informações armazenadas nos blocos
Privacidade e Segurança	Emprego de assinaturas digitais convencionais é vulnerável à computação quântica
	Porcentagem majoritária do poder computacional da rede ser controlado por uma única entidade
Interoperabilidade	Utilização de diferentes mecanismos de consenso, mecanismos de transação e funcionalidades de contratos inteligentes

padrões adotados internacionalmente e devem existir *backups* regulares e políticas claras de retenção de dados para evitar perdas. A conformidade com os padrões também garante a qualidade dos dados capturados. Adicionalmente, deve ser possível realizar auditorias regulares sobre os dados para melhorar a confiabilidade das informações. O uso de sistemas de integração de dados também pode ajudar a conectar diferentes sistemas e bases de dados de saúde, permitindo que os dados sejam compartilhados de maneira segura e eficiente. As APIs, por sua vez, podem ajudar a padronizar a maneira como diferentes sistemas e bases de dados se comunicam e interagem, permitindo o compartilhamento de informações e dados de forma mais fácil e segura. Alguns projetos de pesquisa e ações governamentais em andamento na área de integração de sistemas de saúde são:

- IHE (*Integrating the Healthcare Enterprise*)[39] é uma inciativa global que desenvolve e promove padrões para interoperabilidade de sistemas de saúde, com o objetivo de melhorar a qualidade e a eficiência da assistência à saúde;
- *Common Platform*[40] é um projeto de pesquisa financiado pela União Europeia que visa desenvolver uma plataforma comum para compartilhamento de informações de saúde entre diferentes países europeus. O projeto utiliza padrões de comunicação e segurança para garantir que os dados de saúde sejam compartilhados de maneira segura e eficiente;
- iDASH (*Integrating Data for Analysis, Anonymization, and Sharing*) [Ohno-Machado et al., 2011] é um projeto de pesquisa financiado pelo governo dos Estados Unidos que visa desenvolver uma plataforma para compartilhamento de dados de saúde entre diferentes organizações de saúde. O projeto emprega técnicas de anonimização e segurança para garantir que os dados de saúde sejam compartilhados de maneira segura e protegida;

[39]Disponível em https://www.ihe.net/.
[40]Disponível em https://cordis.europa.eu/project/id/225005.

- RNDS é uma iniciativa governamental brasileira que desenvolve uma plataforma nacional de interoperabilidade para troca de dados em saúde. O objetivo principal é facilitar o acesso e a troca de de dados entre os diferentes sistemas de informação em saúde no Brasil, públicos e privados. A plataforma possibilita a troca segura de dados de saúde de forma padronizada e em conformidade com as políticas de privacidade e segurança vigentes.

Os sistemas tradicionais de saúde também apresentam desafios em relação à **segurança de dado**s. É fundamental garantir a segurança dos dados de saúde, incluindo o acesso seguro e o controle da privacidade do paciente. Isso inclui a implementação de políticas de segurança da informação, criptografia de dados sensíveis, autenticação de usuários e monitoramento contínuo de atividades suspeitas. O uso de ferramentas disponíveis no cotidiano médico fomenta a discussão sobre as práticas de gerenciamento de dados e segurança na área de saúde, ressaltando a necessidade de *software* de fácil manipulação, baixo custo, boa usabilidade, com boas práticas de segurança e agilidade [Araujo Gomes de Castro et al., 2020]. O ambiente médico tem características próprias, complexas e mutáveis com rotinas e procedimentos complexos e com atualizações constantes. A demanda de manipulação dos dados por equipes médica, que podem estar distante geograficamente, inclui o aumento de fluxos de dados que precisam de segurança e demandam criptografia. Além disso, a evolução das tecnologias voltadas para a saúde resulta no aumento da quantidade de dados de saúde digitais disponíveis [Blandford et al., 2020] e, consequentemente, pode haver maior interesse de agentes maliciosos em acessar tais dados. A gestão dos dados deve ser bem estabelecida para assegurar a conformidade com os requisitos regulamentares e as normas vigentes. É fundamental definir papéis e responsabilidades para garantir que apenas quem precisa ter acesso aos dados os acessem de forma segura. Outro desafio é que sistemas de saúde digital agregam complexidade ao ambiente hospitalar, culminando na necessidade de treinamento de equipes multidisciplinares para garantir o acesso seguro e contínuo aos dados sensíveis.

A pandemia da COVID-19 acelerou o processo, incentivando o rápido aumento do uso de tecnologias no cuidado com a saúde. Surtos de doenças anteriores já alertavam para o perigo da sobrecarga de unidades de saúde. A Organização Mundial de Saúde (OMS) atualizou as diretrizes de planejamento operacional durante a pandemia, equilibrando as exigências de responder diretamente à COVID-19, e manter o funcionamento e continuidade de serviços de saúde já existentes, mantendo ainda o padrão de saúde e sanitário, importante no decorrer das ações para mitigar problemas endêmicos e futuros. Nesse cenário, a necessidade de programas que estabelecem a comunicação, assistência e atendimento com qualidade cresceu e a urgência necessária no desenvolvimento trouxe muitos problemas como soluções em *software* que não se comunicam durante o atendimento médico. Os atendimentos via Internet foram feitos realizados, porém em um ambiente desafiador por precisar de vários sistemas que aumentam a complexidade do atendimento médico. Nesse ambiente, a interoperabilidade se torna essencial para o atendimento eficiente do paciente. Há trabalhos e relatos experimentais de como a telessaúde está evoluindo rapidamente, originando inúmeros desafios novos e fomentando desafios antigos. A interoperabilidade, a transparência, a segurança, a rapidez e a disponibilidade são essenciais nos próximos avanços e desenvolvimentos na telessaúde. Assim, as pesquisas em saúde estão fortemente direcionadas para a telessaúde e sistemas inovadores.

A telessaúde constitui uma área estratégica por seu potencial intrínseco de ser fonte geradora de inovações, por demandar e incorporar avanços tecnológicos oriundos de outras áreas, em função da sua natureza interdisciplinar e de suas inter-relações dinâmicas, e pela possibilidade de impulsionar diferentes áreas[41]. Além disso, ressalta-se o aumento da prevalência de doenças crônicas, como insuficiência cardíaca, doença pulmonar e diabetes, que podem ser acompanhadas por meio da telessaúde. Assim, a telessaúde pode melhorar o acesso aos serviços de saúde, reduzir os custos, melhorar os resultados dos pacientes e reduzir a propagação de doenças infecciosas, reduzindo o número de visitas presenciais a instalações de cuidados de saúde. A União Europeia tem feito esforços para implementação e padronização da telessaúde[42]. A interoperabilidade permite que os prestadores de cuidados de saúde partilhem informações sobre os pacientes de forma segura e eficiente, reduzindo o risco de erros e melhorando os resultados dos pacientes. Dentre as novas tecnologias estão a robotização e automatização de laboratórios centrais, multiplicando ao mesmo tempo novos dispositivos para uso periférico e pessoal, com interoperabilidade. Os padrões garantem a interoperabilidade entre componentes heterogêneos e permitem o desenvolvimento de sistemas baseados na descentralização. No Brasil, o Ministério da Saúde, com a Portaria no 2.073 de 2011, define os padrões de interoperabilidade para sistemas de saúde.

Outro desafio relaciona-se à **privacidade** dos dados de saúde. O paradigma da Internet das Coisas, que dissemina e populariza o uso de objetos do cotidiano como câmeras e dispositivos móveis e vestíveis capazes de se comunicarem, permite o monitoramento da saúde dos pacientes. Na China, por exemplo, um sistema que determinava remotamente quem deveria fazer quarentena durante a pandemia de COVID-19 usou dados obtidos por meio de câmeras térmicas em locais públicos com tecnologia de reconhecimento facial e um aplicativo que verificava funções vitais dos usuários diariamente. Vários países europeus usaram redes móveis para informar e identificar pessoas em risco de contaminação [Chén e Roberts, 2021]. Essas aplicações trazem à tona preocupações relacionadas à privacidade dos usuários e à gerência dos dados desses usuários. Especula-se que o uso de dispositivos portáteis e vestíveis continuará a crescer, sendo esses dispositivos cada vez mais usados nos cuidados digitais da saúde [Chén e Roberts, 2021]. Assim, é fundamental buscar soluções que protejam a privacidade dos usuários.

4.7. Considerações Finais

A rápida evolução das ferramentas de Tecnologia da Informação e Comunicação (TIC) no setor de saúde destaca o papel cada vez mais vital dos sistemas eletrônicos e plataformas digitais. A capacidade de compartilhar informações do paciente com eficiência e precisão entre diferentes sistemas médicos tem o potencial de revolucionar a prestação de cuidados de saúde, aprimorar o atendimento ao paciente e impulsionar pesquisas inovadoras. No entanto, o desafio reside na complexidade inerente e na diversidade dos formatos de dados usados em vários sistemas médicos, dificultando a interoperabilidade

[41] Disponível em https://www.who.int/fr/news/item/30-03-2020-who-releases-guidelines-to-help-countries-maintain-essential-health-services-during-the-covid-19-pandemic.

[42] Disponível em https://dialnet.unirioja.es/servlet/articulo?codigo=5635387.

crucial para atingir esses objetivos transformadores. Como resultado, a complexidade do sistema médico impede o acesso fácil ao histórico médico completo do paciente, quando necessário, levando à perda ou coleta repetitiva de informações, dificultando o diagnóstico e o tratamento e impactando negativamente a jornada do paciente.

Os ambientes eletrônicos de saúde facilitam o acesso a dados distribuídos, armazenando os dados do paciente em Registros Médicos Eletrônicos (EMRs) padronizados. Os EMRs contêm informações pessoais privadas sobre o paciente, incluindo diagnósticos e tratamentos, e são normalmente distribuídos entre hospitais e clínicas que trataram o paciente pelo menos uma vez na vida. Os EMRs permitem acesso rápido e padronizado aos dados do paciente e permitem a integração do atendimento ao paciente entre equipes médicas e diferentes unidades de saúde, garantindo que diferentes níveis de atendimento tenham acesso às informações médicas relevantes de cada paciente. Os EMRs são altamente sensíveis e confidenciais. Contudo, o compartilhamento ocorre, por vezes, sem o consentimento do paciente entre entidades não confiáveis, como profissionais de saúde, farmácias, familiares e outros médicos. Embora sistemas institucionalizados seguros sejam usados para compartilhar dados do paciente quando necessário, dados sensíveis também são compartilhados usando meios de comunicação informais e inseguros.

No contexto da pandemia de COVID-19, a necessidade de agilizar o atendimento e o fluxo de informações entre pacientes, médicos e instituições de saúde tornou-se ainda mais crucial. Os registros de pacientes ganham importância crescente em termos de saúde pública e dados sobre diagnósticos e medicamentos prescritos podem ser usados para identificar indivíduos em risco de doenças como a COVID-19. A maior disponibilidade de dados do paciente em formato eletrônico é de grande relevância para a tomada de decisões e continuidade do cuidado tanto no setor público quanto no privado, principalmente com troca de informações entre as duas esferas. A detecção precoce de surtos de doenças é crucial para coordenar as políticas de saúde pública e os esforços de prevenção em nível nacional de forma eficiente. O compartilhamento eficiente também beneficia os pacientes, pois permite que eles acessem suas próprias informações a qualquer momento, como resultados laboratoriais e de imagem, e facilita a portabilidade desses dados para outros profissionais de saúde. A comunicação eficiente e automatizada entre pacientes e equipes médicas promove a transparência, aumenta a satisfação do paciente e garante o acesso universal aos dados. No entanto, ainda há desafios a serem enfrentados. A maioria dos sistemas de EMR é baseada em arquiteturas cliente-servidor centralizadas, que apresentam desafios de privacidade e segurança. As vulnerabilidades do sistema podem levar a falhas e criar oportunidades para que invasores cibernéticos comprometam os dados do paciente. Além disso, os registros dos pacientes geralmente são fragmentados em bancos de dados locais, impedindo a consolidação do histórico médico eletrônico do paciente. A padronização dos formatos de dados é essencial para alcançar a interoperabilidade no setor de saúde. A padronização envolve o estabelecimento de uma linguagem comum para troca e interpretação de dados médicos, permitindo que diferentes sistemas se comuniquem entre si.

A tecnologia de cadeia de blocos é uma candidata à interface de padronização e interoperação entre sistemas de saúde. Embora tenha potencial para ser usada no setor de saúde, ela ainda é considerada uma tecnologia complementar aos sistemas legados, e não uma substituta. A integração da tecnologia de cadeia de blocos na área da saúde apresenta

vários desafios técnicos, incluindo escalabilidade, usabilidade, irreversibilidade, privacidade e segurança e interoperabilidade. A escalabilidade é um obstáculo potencial para a adoção generalizada de cadeias de blocos públicos no setor de saúde. As cadeias de blocos públicas têm limitações em termos de velocidade de processamento de transações e tempo de validação de blocos, o que pode afetar adversamente a análise de exames médicos e o diagnóstico oportuno. A usabilidade é outro desafio nos sistemas de saúde baseados em cadeia de blocos. A complexidade de gerenciamento e manutenção desses sistemas, juntamente com a escassez de profissionais qualificados com experiência em saúde e TIC, muitas vezes resulta em sistemas com baixa usabilidade. A característica de imutabilidade na cadeia de blocos promove desafios em termos de manipulação de dados. Depois que os dados são gravados em um bloco, eles não podem ser modificados ou excluídos, o que pode ser problemático para armazenar dados temporários ou não críticos. Além disso, a exposição de chaves privadas pode comprometer permanentemente a privacidade do paciente. Privacidade e segurança são preocupações críticas em sistemas de saúde baseados em cadeias de blocos. A transparência das redes de cadeias de blocos e a dependência de intermediários para acessar informações pessoais de saúde podem comprometer a privacidade do paciente. Por fim, a interoperabilidade é essencial para a troca de informações entre sistemas heterogêneos na área da saúde. A falta de padronização e a presença de várias redes cadeias de blocos com diferentes mecanismos de consenso, mecanismos de transação e funcionalidades de contratos inteligentes dificultam a interoperabilidade.

Diversos atores no mercado de saúde digital identificam a falta de interoperabilidade entre os sistemas de informações de saúde, o que compromete a segurança dos dados. Esse fato também restringe o acesso às informações, reduzindo a integração entre registros dispersos por clínicas e hospitais. Esse capítulo apresentou as possibilidades de integração e padrões de representação de dados em saúde. Espera-se que nos próximos anos, projetos de pesquisa e produtos comerciais foquem a missão vital de padronização e integração em sistemas de compartilhamento de registros médicos eletrônicos, pois são desafios que detêm a oportunidade de revolucionar a saúde, ampliar os resultados positivos aos pacientes e moldar um futuro em que a colaboração e a inovação prosperem.

Referências

[Abomhara e Ben Lazrag, 2016] Abomhara, M. e Ben Lazrag, M. (2016). UML/OCL-based modeling of work-based access control policies for collaborative healthcare systems. Em *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, p. 1–6.

[Abomhara et al., 2016] Abomhara, M., Yang, H. e Køien, G. M. (2016). Access control model for cooperative healthcare environments: Modeling and verification. Em *2016 IEEE International Conference on Healthcare Informatics (ICHI)*, p. 46–54. IEEE.

[Agrawal et al., 2022] Agrawal, D., Minocha, S., Namasudra, S. e Gandomi, A. H. (2022). A robust drug recall supply chain management system using hyperledger blockchain ecosystem. *Computers in biology and medicine*, 140:105100.

[Al Omar et al., 2017] Al Omar, A., Rahman, M. S., Basu, A. e Kiyomoto, S. (2017). MediBChain: A blockchain based privacy preserving platform for healthcare data.

Em *Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2017 International Workshops, Guangzhou, China, December 12-15, 2017, Proceedings 10*, p. 534–543. Springer.

[Albeyatt, 2018] Albeyatt, A. (2018). Medicalchain white paper 2.1. Relatório técnico, MedChain White Paper 2.1.

[Anderson, 2018] Anderson, J. (2018). Securing, standardizing, and simplifying electronic health record audit logs through permissioned blockchain technology. *UNTHRR*.

[Araujo Gomes de Castro et al., 2020] Araujo Gomes de Castro, F., Oliveira dos Santos, Á., Valadares Labanca Reis, G., Brandão Viveiros, L., Hespanhol Torres, M. e de Oliveira Junior, P. P. (2020). Telemedicina rural e COVID-19: ampliando o acesso onde a distância já era regra. *Revista Brasileira de Medicina de Família e Comunidade*, 15(42):2484.

[Azaria et al., 2016] Azaria, A., Ekblaw, A., Vieira, T. e Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. Em *2016 2nd international conference on open and big data (OBD)*, p. 25–30. IEEE.

[Blandford et al., 2020] Blandford, A., Wesson, J., Amalberti, R., AlHazme, R. e Allwihan, R. (2020). Opportunities and challenges for telehealth within, and beyond, a pandemic. *The Lancet Global Health*, 8(11):e1364–e1365.

[Byun et al., 2005] Byun, J.-W., Bertino, E. e Li, N. (2005). Purpose based access control of complex data for privacy protection. Em *Proceedings of the Tenth ACM Symposium on Access Control Models and Technologies*, SACMAT '05, p. 102–110, New York, NY, USA. Association for Computing Machinery.

[Cachin e Vukolic, 2017] Cachin, C. e Vukolic, M. (2017). Blockchain Consensus Protocols in the Wild (Keynote Talk). Em Richa, A. W., editor, *31st International Symposium on Distributed Computing (DISC 2017)*, volume 91 of *Leibniz International Proceedings in Informatics (LIPIcs)*, p. 1:1–1:16, Dagstuhl, Germany. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[Carrara et al., 2020] Carrara, G. R., Burle, L. M., Medeiros, D. S. V., de Albuquerque, C. V. N. e Mattos, D. M. F. (2020). Consistency, availability, and partition tolerance in blockchain: a survey on the consensus mechanism over peer-to-peer networking. *Annals of Telecommunications*, 75(3):163–174.

[Cetic.br, 2020] Cetic.br (2020). *Pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros : TIC Saúde 2019*. Núcleo de Informação e Coordenação do Ponto BR (NIC.br).

[Chowdhury et al., 2019] Chowdhury, M. J. M., Ferdous, M. S., Biswas, K., Chowdhury, N., Kayes, A., Alazab, M. e Watters, P. (2019). A comparative analysis of distributed ledger technology platforms. *IEEE Access*, 7:167930–167943.

[Christidis e Devetsikiotis, 2016] Christidis, K. e Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303.

[Chén e Roberts, 2021] Chén, O. Y. e Roberts, B. (2021). Personalized health care and public health in the digital age. *Frontiers in Digital Health*, 3.

[Dagher et al., 2018] Dagher, G. G., Mohler, J., Milojkovic, M. e Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable cities and society*, 39:283–297.

[Dang et al., 2018] Dang, L., Dong, M., Ota, K., Wu, J., Li, J. e Li, G. (2018). Resource-efficient secure data sharing for information centric e-health system using fog computing. Em *2018 IEEE International Conference on Communications (ICC)*, p. 1–6. IEEE.

[Daraghmi et al., 2019] Daraghmi, E.-Y., Daraghmi, Y.-A. e Yuan, S.-M. (2019). MedChain: a design of blockchain-based system for medical records access and permissions management. *IEEE Access*, 7:164595–164613.

[De Aguiar et al., 2020] De Aguiar, E. J., Faiçal, B. S., Krishnamachari, B. e Ueyama, J. (2020). A survey of blockchain-based strategies for healthcare. *ACM Comput. Surv.*, 53(2).

[de Oliveira et al., 2019] de Oliveira, M. T., Reis, L. H., Carrano, R. C., Seixas, F. L., Saade, D. C., Albuquerque, C. V., Fernandes, N. C., Olabarriaga, S. D., Medeiros, D. S. e Mattos, D. M. (2019). Towards a blockchain-based secure electronic medical record for healthcare applications. Em *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, p. 1–6. IEEE.

[de Oliveira et al., 2023] de Oliveira, M. T., Verginadis, Y., Reis, L. H., Psarra, E., Patiniotakis, I. e Olabarriaga, S. D. (2023). AC-ABAC: Attribute-based access control for electronic medical records during acute care. *Expert Systems with Applications*, 213:119271.

[DICOM, 2023] DICOM, D. S. C. (2023). Dicom ps3.1 2023b. Relatório técnico, DICOM Standards Committee.

[Dubovitskaya et al., 2017] Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M. e Wang, F. (2017). Secure and trustable electronic medical records sharing using blockchain. Em *AMIA annual symposium proceedings*, volume 2017, p. 650. American Medical Informatics Association.

[Engelhardt, 2017] Engelhardt, M. A. (2017). Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. *Technology Innovation Management Review*, 7(10).

[Fan et al., 2018] Fan, K., Wang, S., Ren, Y., Li, H. e Yang, Y. (2018). MedBlock: Efficient and secure medical data sharing via blockchain. *Journal of medical systems*, 42:1–11.

[Ghorbel et al., 2021] Ghorbel, A., Ghorbel, M. e Jmaiel, M. (2021). Accountable privacy preserving attribute-based access control for cloud services enforced using block-

chain. *International Journal of Information Security*, p. 1–20.

[Guo et al., 2018] Guo, R., Shi, H., Zhao, Q. e Zheng, D. (2018). Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. *IEEE access*, 6:11676–11686.

[Haas et al., 2011] Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N. e Müller, G. (2011). Aspects of privacy for electronic health records. *International Journal of Medical Informatics*, 80(2):e26–e31. Special Issue: Security in Health Information Systems.

[Harrison et al., 2021] Harrison, J. E., Weber, S., Jakob, R. e Chute, C. G. (2021). ICD-11: an international classification of diseases for the twenty-first century. *BMC Medical Informatics and Decision Making*, 21(6).

[HL7, 2015] HL7, H. L. S. I. (2015). Hl7 implementation guide for cda® release 2: Consolidated cda templates for clinical notes (us realm) draft standard for trial use release 2.1. Relatório técnico, Health Level Seven International.

[Hurst et al., 2022] Hurst, W., Tekinerdogan, B., Alskaif, T., Boddy, A. e Shone, N. (2022). Securing electronic health records against insider-threats: A supervised machine learning approach. *Smart Health*, 26:100354.

[Jacquemard et al., 2020] Jacquemard, T., Doherty, C. P. e Fitzsimons, M. B. (2020). Examination and diagnosis of electronic patient records and their associated ethics: a scoping literature review. *BMC Medical Ethics*, 21(1):76.

[Janett e Yeracaris, 2020] Janett, R. S. e Yeracaris, P. P. (2020). Electronic medical records in the american health system: challenges and lessons learned. *Ciencia & saude coletiva*, 25:1293–1304.

[Jiang et al., 2018] Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M. e He, J. (2018). Blochie: a blockchain-based platform for healthcare information exchange. Em *2018 ieee international conference on smart computing (smartcomp)*, p. 49–56. IEEE.

[Kaur e Gandhi, 2020] Kaur, G. e Gandhi, C. (2020). Scalability in blockchain: Challenges and solutions. Em *Handbook of Research on Blockchain Technology*, p. 373–406. Elsevier.

[Larrucea et al., 2020] Larrucea, X., Moffie, M., Asaf, S. e Santamaria, I. (2020). Towards a GDPR compliant way to secure european cross border healthcare industry 4.0. *Computer Standards and Interfaces*, 69:103408.

[Lee et al., 2021] Lee, T.-F., Chang, I.-P. e Kung, T.-S. (2021). Blockchain-based healthcare information preservation using extended chaotic maps for HIPAAprivacy/security regulations. *Applied Sciences*, 11(22).

[Lesk, 2013] Lesk, M. (2013). Electronic medical records: Confidentiality, care, and epidemiology. *IEEE security & privacy*, 11(6):19–24.

[Liang et al., 2017] Liang, X., Zhao, J., Shetty, S., Liu, J. e Li, D. (2017). Integrating

blockchain for data sharing and collaboration in mobile healthcare applications. Em *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)*, p. 1–5. IEEE.

[Lo et al., 2017] Lo, S. K., Xu, X., Chiam, Y. K. e Lu, Q. (2017). Evaluating suitability of applying blockchain. Em *2017 22nd international conference on engineering of complex computer systems (ICECCS)*, p. 158–161. IEEE.

[Luh e Yen, 2020] Luh, F. e Yen, Y. (2020). Cybersecurity in science and medicine: Threats and challenges. *Trends in Biotechnology*, 38(8):825–828.

[Maani et al., 2011] Maani, R., Camorlinga, S. e Arnason, N. (2011). A parallel method to improve medical image transmission. *Journal of Digital Imaging*, 25(1):101–109.

[Maesa et al., 2019] Maesa, D. D. F., Mori, P. e Ricci, L. (2019). A blockchain based approach for the definition of auditable access control systems. *Computers & Security*, 84:93–119.

[Makary e Daniel, 2016] Makary, M. A. e Daniel, M. (2016). Medical error—the third leading cause of death in the US. *Bmj*, 353.

[Massad et al., 2003] Massad, E., Marin, H. d. F. e Azevedo Neto, R. S. d., editors (2003). *O prontuário eletrônico do paciente na assistência, informação e conhecimento médico*. USP, São Paulo.

[Mattos et al., 2018] Mattos, D. M., Medeiros, D. S., Fernandes, N. C., de Oliveira, M. T., Carrara, G. R., Soares, A. A., Magalhães, L. C. S., Passos, D., Carrano, R. C., Moraes, I. M. et al. (2018). Blockchain para segurança em redes elétricas inteligentes: Aplicações, tendências e desafios. *Sociedade Brasileira de Computação*.

[Mettler, 2016] Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. Em *2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom)*, p. 1–3. IEEE.

[Nakamoto, 2008] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*, p. 21260.

[Namasudra et al., 2022] Namasudra, S., Sharma, P., Crespo, R. G. e Shanmuganathan, V. (2022). Blockchain-based medical certificate generation and verification for IoT-based healthcare systems. *IEEE Consumer Electronics Magazine*.

[Nazerian et al., 2019] Nazerian, F., Motameni, H. e Nematzadeh, H. (2019). Emergency role-based access control E-RBAC and analysis of model specifications with alloy. *Journal of information security and applications*, 45:131–142.

[Ohno-Machado et al., 2011] Ohno-Machado, L., Bafna, V., Boxwala, A. A., Chapman, B. E., Chapman, W. W., Chaudhuri, K., Day, M. E., Farcas, C., Heintzman, N. D., Jiang, X., Kim, H., Kim, J., Matheny, M. E., Resnic, F. S., Vinterbo, S. A., e the iDASH team (2011). iDASH: integrating data for analysis, anonymization, and sharing. *Journal of the American Medical Informatics Association*, 19(2):196–201.

[Patel, 2019] Patel, V. (2019). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health informatics journal*, 25(4):1398–1411.

[Peleg et al., 2008] Peleg, M., Beimel, D., Dori, D. e Denekamp, Y. (2008). Situation-based access control: Privacy management via modeling of patient data access scenarios. *Journal of Biomedical Informatics*, 41(6):1028–1040.

[Pustokhin et al., 2021] Pustokhin, D. A., Pustokhina, I. V. e Shankar, K. (2021). *Challenges and Future Work Directions in Healthcare Data Management Using Blockchain Technology*, p. 253–267. Springer Singapore, Singapore.

[Rahman et al., 2021] Rahman, A., Hossain, M. S., Alrajeh, N. A. e Alsolami, F. (2021). Adversarial examples—security threats to COVID-19 deep learning systems in medical IoT devices. *IEEE Internet of Things Journal*, 8(12):9603–9610.

[Rebello et al., 2019] Rebello, G., Camilo, G., Silva, L., Souza, L., Guimarães, L., Alchieri, E., Greve, F. e Duarte, O. (2019). Correntes de blocos: Algoritmos de consenso e implementação na plataforma hyperledger fabric. *Sociedade Brasileira de Computação*.

[Rouhani et al., 2021] Rouhani, S., Belchior, R., Cruz, R. S. e Deters, R. (2021). Distributed attribute-based access control system using permissioned blockchain. *World Wide Web*, p. 1–28.

[Salim e Park, 2023] Salim, M. M. e Park, J. H. (2023). Federated learning-based secure electronic health record sharing scheme in medical informatics. *IEEE Journal of Biomedical and Health Informatics*, 27(2):617–624.

[Sandgaard e Wishstar, 2018] Sandgaard, J. e Wishstar, S. (2018). Medchain white paper 2.1. Relatório técnico, MedChain White Paper 2.1.

[Santos et al., 2022] Santos, S. d. L. V. d., Zara, A. L. d. S. A., Lucena, F. N. d., Ribeiro-Rotta, R. F., Braga, R. D., Amaral, R. G., Pedrosa, S. M. e Kudo, T. N. (2022). *Rede Nacional de Dados em Saúde: o que precisamos saber?* Cegraf UFG.

[Savage, 2014] Savage, R. (2014). Hl7 version 2.5.1, implementation guide for immunization messaging. Relatório técnico, Centers for Disease Control and Prevention.

[Seol et al., 2018] Seol, K., Kim, Y.-G., Lee, E., Seo, Y.-D. e Baik, D.-K. (2018). Privacy-preserving attribute-based access control model for XML-based electronic health record system. *IEEE Access*, 6:9114–9128.

[Siyal et al., 2019] Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A. e Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography*, 3(1):3.

[Stoeger e Schmidhuber, 2020] Stoeger, K. e Schmidhuber, M. (2020). The use of data from electronic health records in times of a pandemic—a legal and ethical assessment. *Journal of Law and the Biosciences*, 7(1):lsaa041.

[Tanwar et al., 2020] Tanwar, S., Parekh, K. e Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, 50:102407.

[Tormo et al., 2013] Tormo, G. D., Mármol, F. G., Girao, J. e Pérez, G. M. (2013). Identity management–in privacy we trust: bridging the trust gap in ehealth environments. *IEEE security & privacy*, 11(6):34–41.

[Tribunal de Contas da União (TCU), 2020] Tribunal de Contas da União (TCU) (2020). Levantamento de aplicações blockchain: Aplicações blockchain no setor pública do brasil (apêndice 1). Sumário executivo, Tribunal de Contas da União (TCU).

[Tschorsch e Scheuermann, 2016] Tschorsch, F. e Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, 18(3):2084–2123.

[Uddin et al., 2018] Uddin, M. A., Stranieri, A., Gondal, I. e Balasubramanian, V. (2018). Continuous patient monitoring with a patient centric agent: A block architecture. *IEEE Access*, 6:32700–32726.

[WHO, 2022] WHO, G. W. H. O. (2022). International classification of diseases, eleventh revision ICD-11. Relatório técnico, World Health Organization.

[Xia et al., 2017] Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X. e Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*, 5:14757–14767.

[Xu et al., 2017] Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C. e Rimba, P. (2017). A taxonomy of blockchain-based systems for architecture design. Em *2017 IEEE international conference on software architecture (ICSA)*, p. 243–252. IEEE.

[Yaqoob et al., 2022] Yaqoob, I., Salah, K., Jayaraman, R. e Al-Hammadi, Y. (2022). Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. *Neural Computing and Applications*, 34.

[Yu et al., 2020] Yu, G., Wang, X., Yu, K., Ni, W., Zhang, J. A. e Liu, R. P. (2020). Survey: Sharding in blockchains. *IEEE Access*, 8:14155–14181.

[Yue et al., 2016] Yue, X., Wang, H., Jin, D., Li, M. e Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems*, 40:1–8.

[Zhang et al., 2018] Zhang, P., White, J., Schmidt, D. C., Lenz, G. e Rosenbloom, S. T. (2018). FHIRChain: applying blockchain to securely and scalably share clinical data. *Computational and structural biotechnology journal*, 16:267–278.

[Zhang e Poslad, 2018] Zhang, X. e Poslad, S. (2018). Blockchain support for flexible queries with granular access control to electronic medical records EMR. Em *2018 IEEE International conference on communications (ICC)*, p. 1–6. IEEE.

