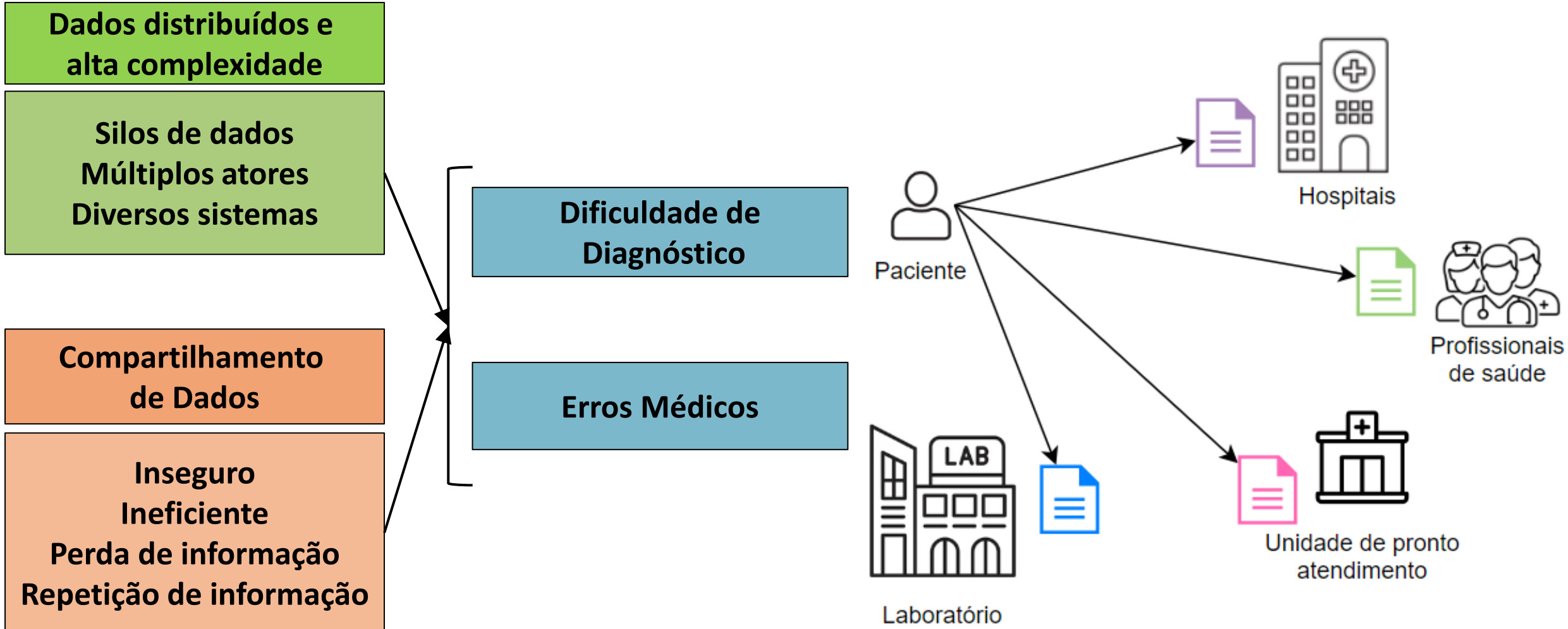


Padrões e Soluções para Armazenamento, Compartilhamento e Estruturação de Dados em Saúde Digital: Privacidade, Integração e Desafios

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 (TUDelft), Rafael Valle (RNP),
Dianne S. V. Medeiros (UFF), Diogo M. F. Mattos (UFF)

Sistemas Médicos Tradicionais

Problemas



Informatização da Saúde

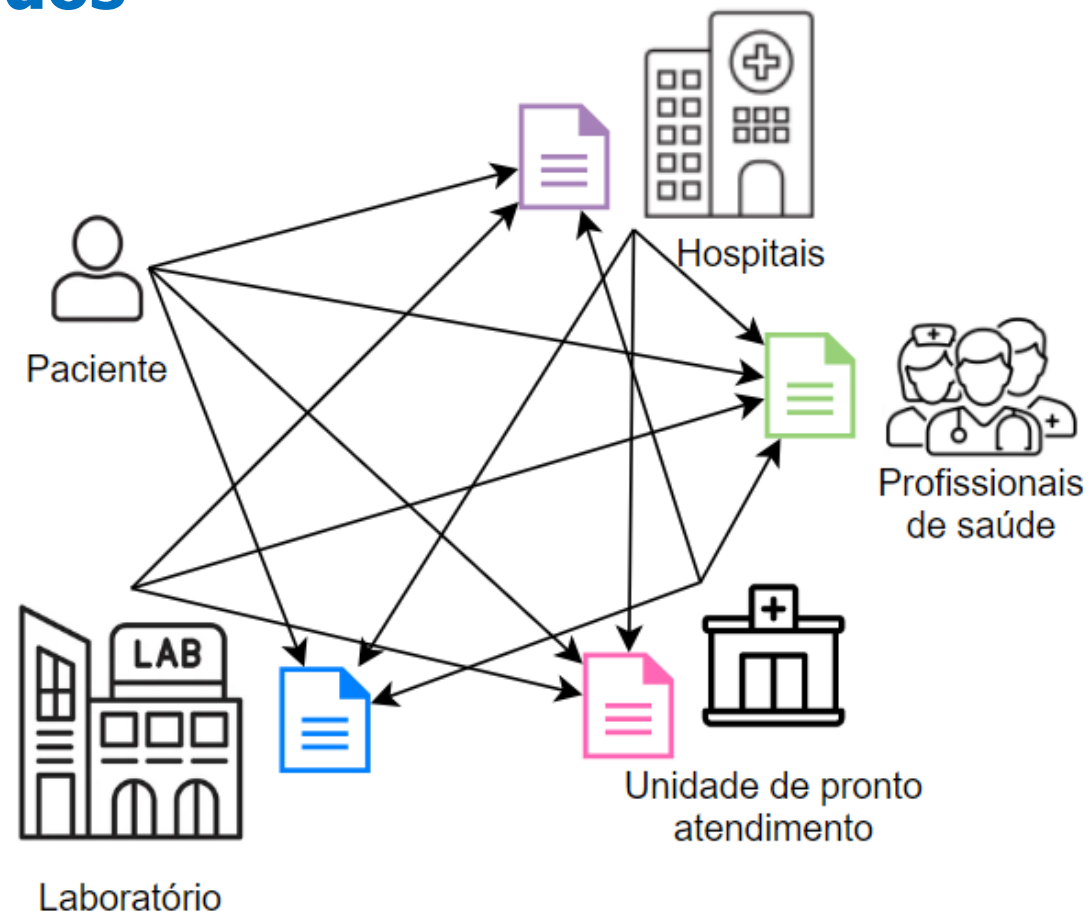
Vantagens

- **Facilita o acesso aos dados distribuídos**

- Histórico completo de saúde do paciente
- Diagnóstico precoce
- Tratamento mais efetivo

- **Registros médicos eletrônicos**
(*Electronic Medical Records – EMRs*)

- Agilidade no atendimento
- Maior disponibilidade dos dados
- Continuidade do tratamento
 - Setores públicos e privados
- Integração do cuidado
 - Compartilhamento entre membros de equipes



- **Informações pessoais privadas**

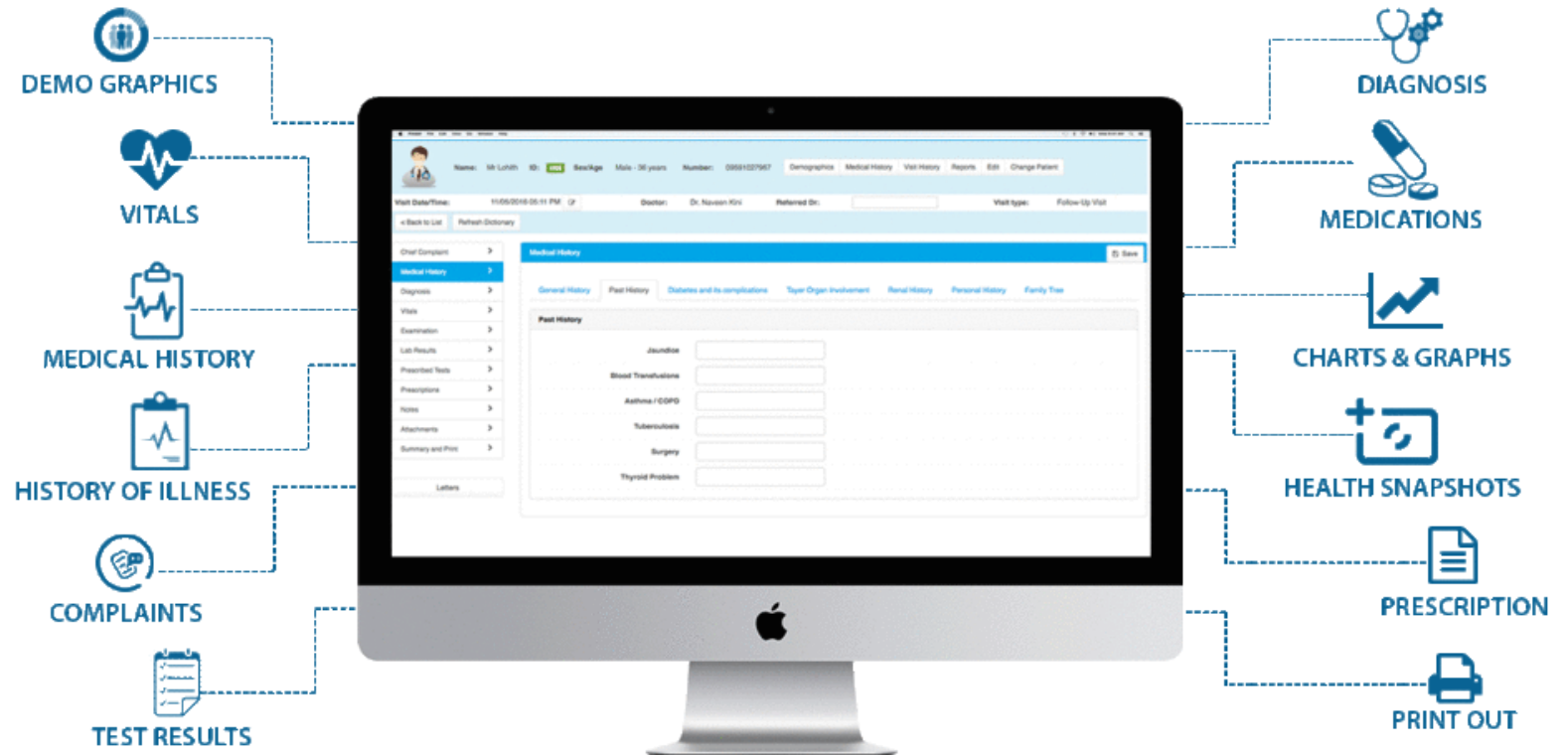
- Diagnósticos e tratamentos
- Identificação do paciente
- Anamnese e exame físico
- Exames

- **Facilidade de acesso**

- **Histórico do paciente**

- **Compartilhamento de informações**

- Requer consentimento do paciente
 - Informações sensíveis

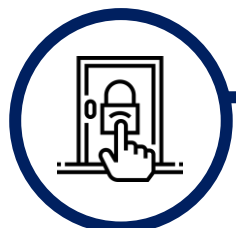


- **Compartilhamento de informações**
 - Sem consentimento
 - **Entidades não confiáveis**
 - Profissionais de saúde, familiares, farmácias, ...
 - **Inseguro**
 - Imediatismo e simplicidade
 - Meios de comunicação não institucionalizados e não confiáveis
- **Multiplicidade de sistemas**
 - **Fragmentação dos registros** em bancos de dados locais
 - Impede consolidação do prontuário do paciente
 - **Diversidade de formatos** de dados
 - Dificulta a interoperabilidade

Registros Médicos Eletrônicos

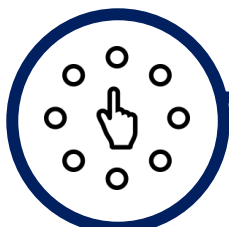
Problemas

- Desafios relacionados à **interoperabilidade** e à **proteção da privacidade** dos pacientes



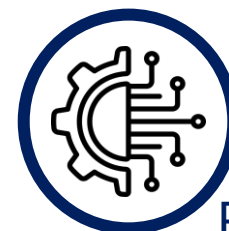
Gerenciamento de Identidade e Controle de Acesso

Comprometido diante da **cultura de compartilhamento de senhas** e **gerenciamento centralizado** dos dados



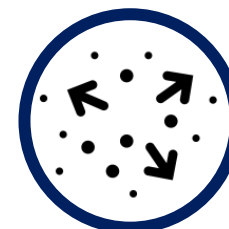
Diversidade de Sistemas Disponíveis no Mercado

Dificultando a escolha, integração e operação devido a **falta de padronização**



Resistência à tecnologia

Preferência por preenchimento manual de registros e prontuários está relacionada à **praticidade e ao receio de instabilidade**



Pulverização das Informações dos Pacientes

Derivada da **multiplicidade de ferramentas independentes**, uma para cada especialidade

- **Padronização do formato de dados**

- Linguagem comum para a troca e interpretação de dados médicos
- Comunicação entre sistemas distintos



- **Controle de acesso**

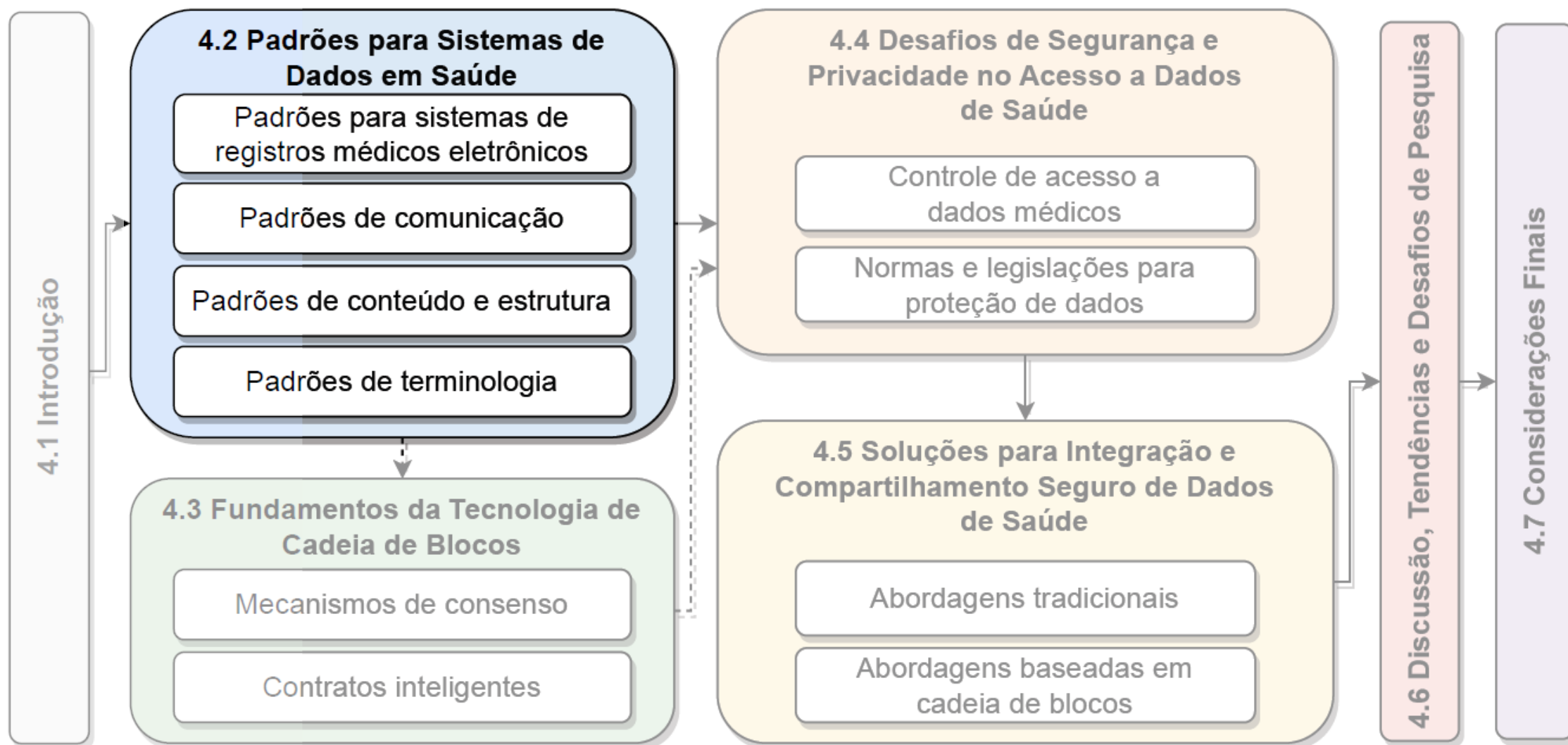
- Limitação de acesso a informações por meio de políticas



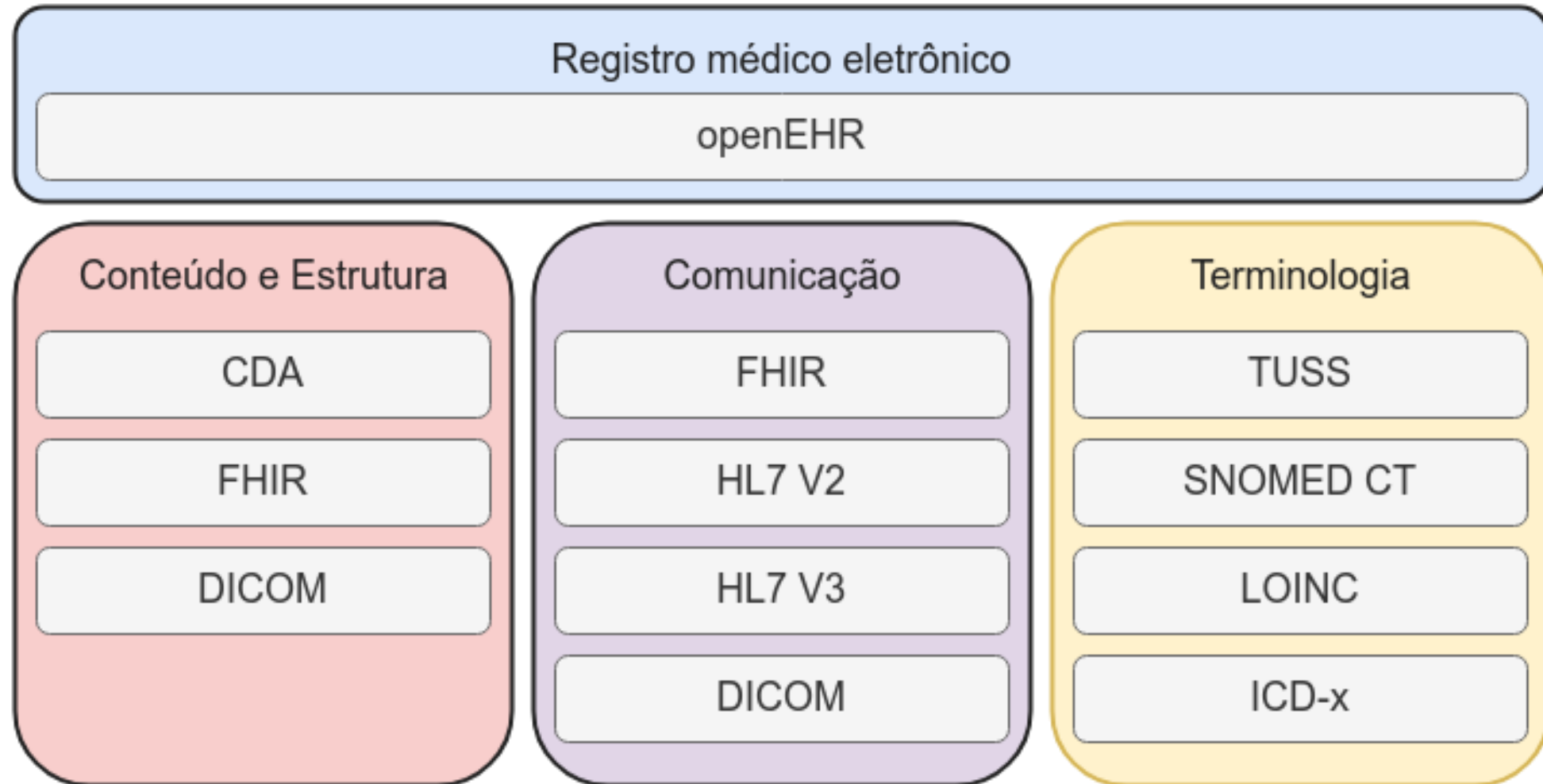
- **Rastreabilidade e descentralização**

- Melhoria de disponibilidade
- Capacidade de auditoria





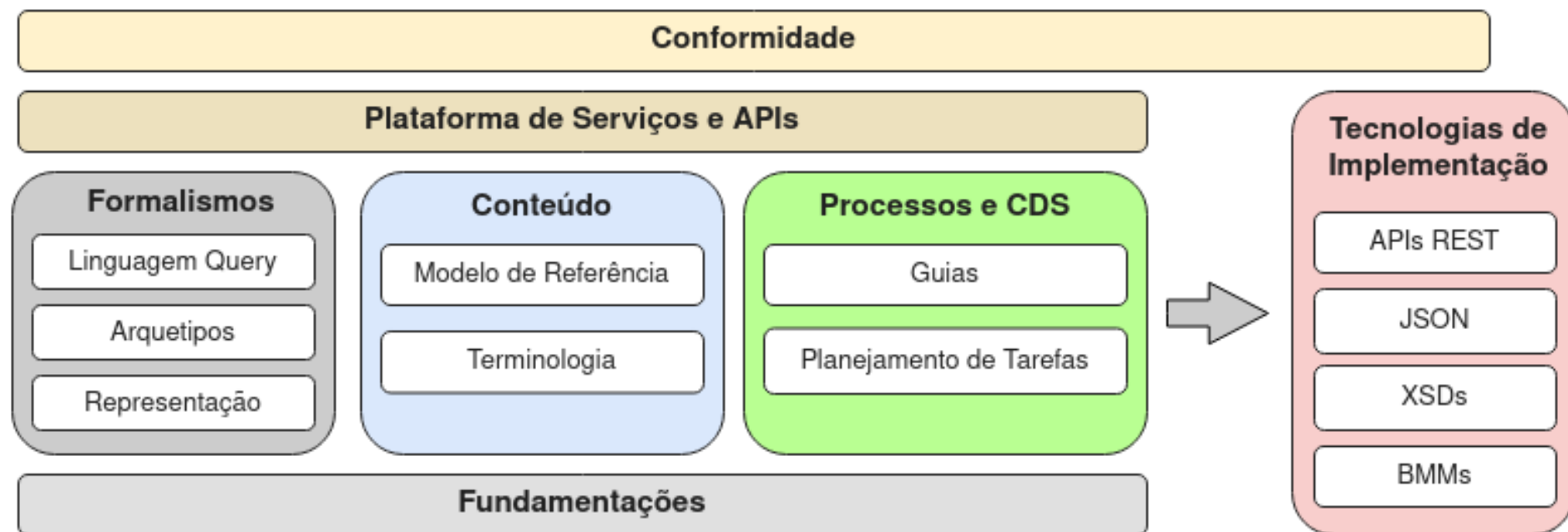
- **Padronização para Sistemas de Registros Médicos Eletrônicos**
 - Definição de modelo de referência para desenvolvimento de sistemas de registros médicos eletrônicos
- **Padronização para Conteúdo e Estrutura**
 - Definição das informações coletadas, armazenadas, processadas e compartilhadas em sistemas de saúde e formato dessas informações
- **Padronização para Comunicação**
 - Definição de conteúdo, formato e protocolo para a transação de registros médicos eletrônicos
- **Padronização para Terminologia**
 - Definição do nome de doenças, procedimentos e situações clínicas visando uma forma de representação unificada



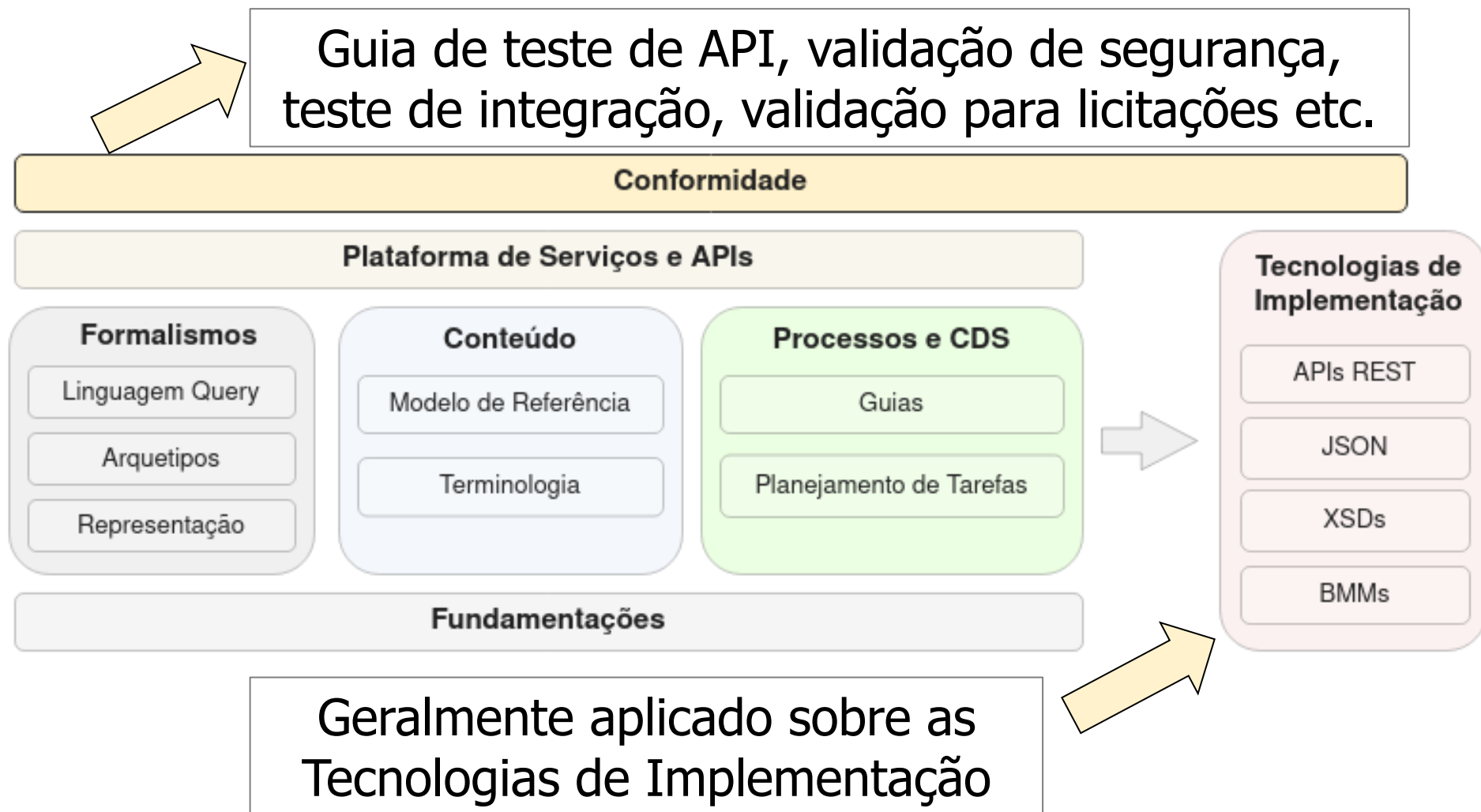
- Proposta
 - Definir **modelos de referência** para sistemas de registros médicos eletrônicos
- Objetivo
 - Promover a **interoperabilidade** entre diferentes sistemas de saúde
 - Definir os padrões a serem utilizados por cada **componente** de um sistema

- **Modelo de referência** genérico e **duas arquiteturas** de sistemas baseadas nesse modelo
 - Especificação dos **componentes dos modelos de referência**
 - Baseadas em uma abordagem de separação de papéis
- **Profissionais da saúde definem e validam os modelos** de dados a serem armazenados
- **Desenvolvedores implementam** as funcionalidades baseadas nas definições dos profissionais da saúde

Modelo de Referência Genérico openEHR



Modelo de Referência Genérico openEHR



Modelo de Referência Genérico openEHR

Componente voltado para a definição dos recursos que focam a interoperabilidade da aplicação

Conformidade

Plataforma de Serviços e APIs

Formalismos

Linguagem Query

Arquetipos

Representação

Conteúdo

Modelo de Referência

Terminologia

Processos e CDS

Guias

Planejamento de Tarefas

Fundamentações

Tecnologias de Implementação

APIs REST

JSON

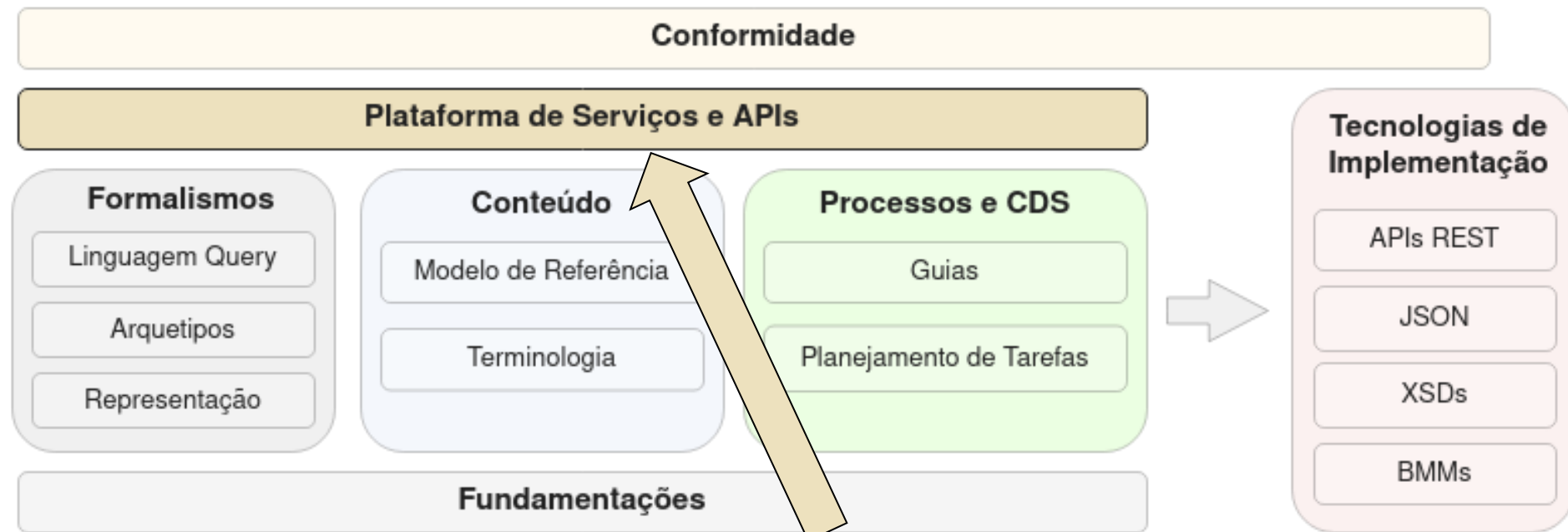
XSDs

BMMs

Especifica padrões usados para comunicação (APIs REST), formato de dados (JSON e XSDs), e representação das classes da interface (BMMs)

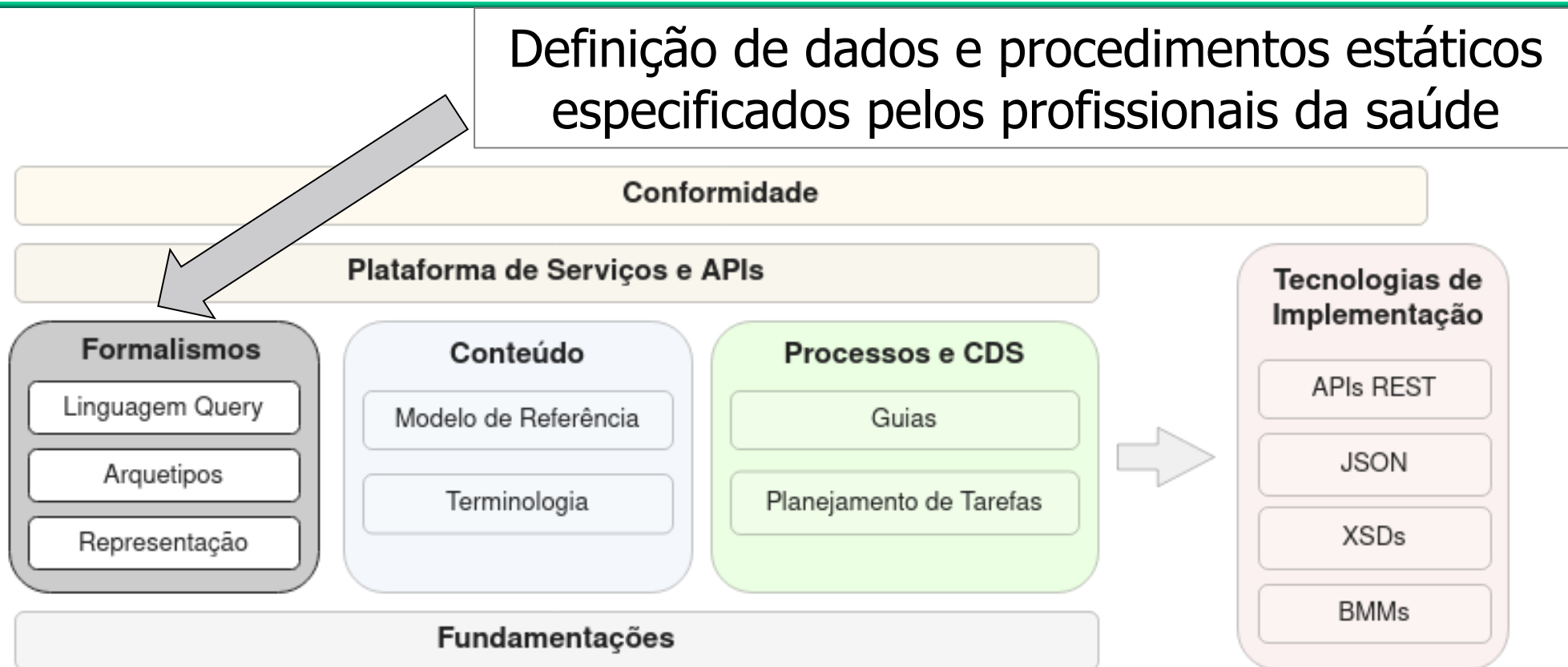
Modelo de Referência Genérico

openEHR



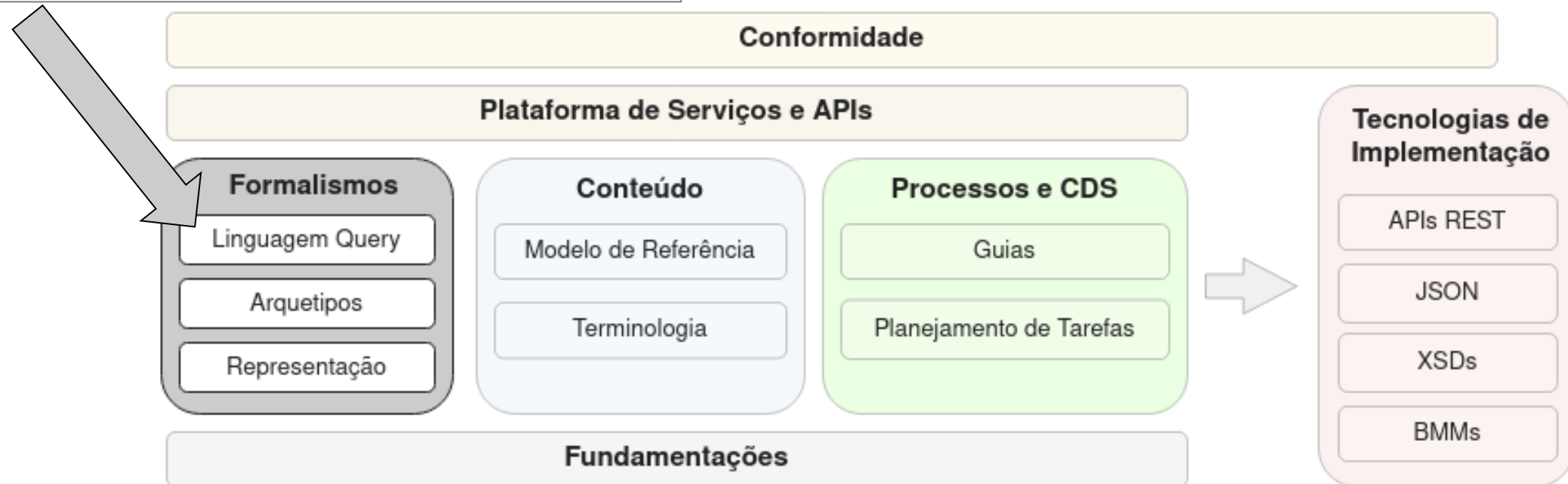
APIs formais abstratas que definem as interfaces de integração do openEHR

Modelo de Referência Genérico openEHR

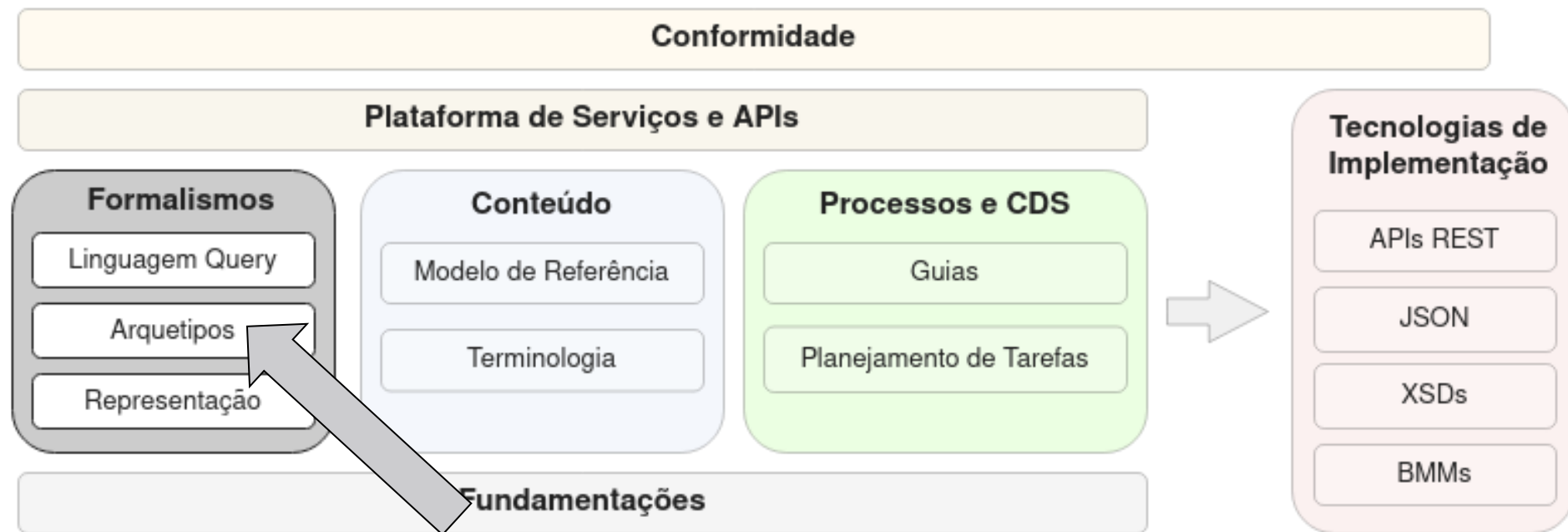


Modelo de Referência Genérico openEHR

Linguagem Query para consulta
na base de arquétipos



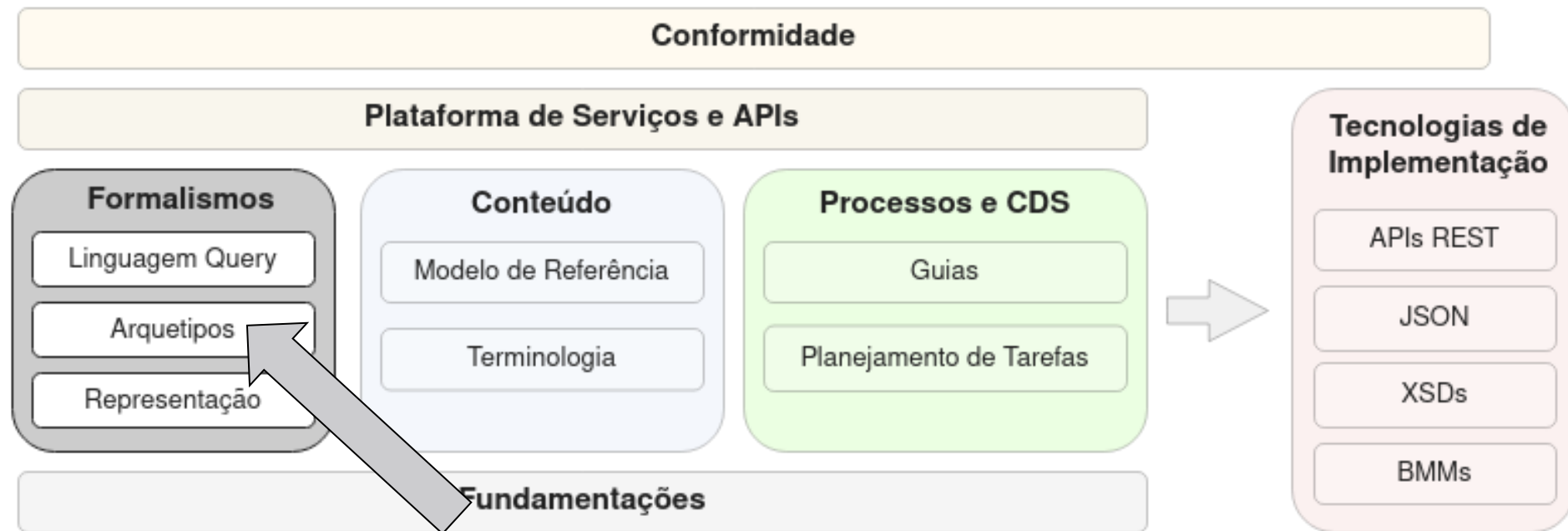
Modelo de Referência Genérico openEHR



Conceito clínico consolidado que define a estrutura de um objeto que pode ser reutilizado (Ex.: "pressão sanguínea", "endereço", "histórico familiar")

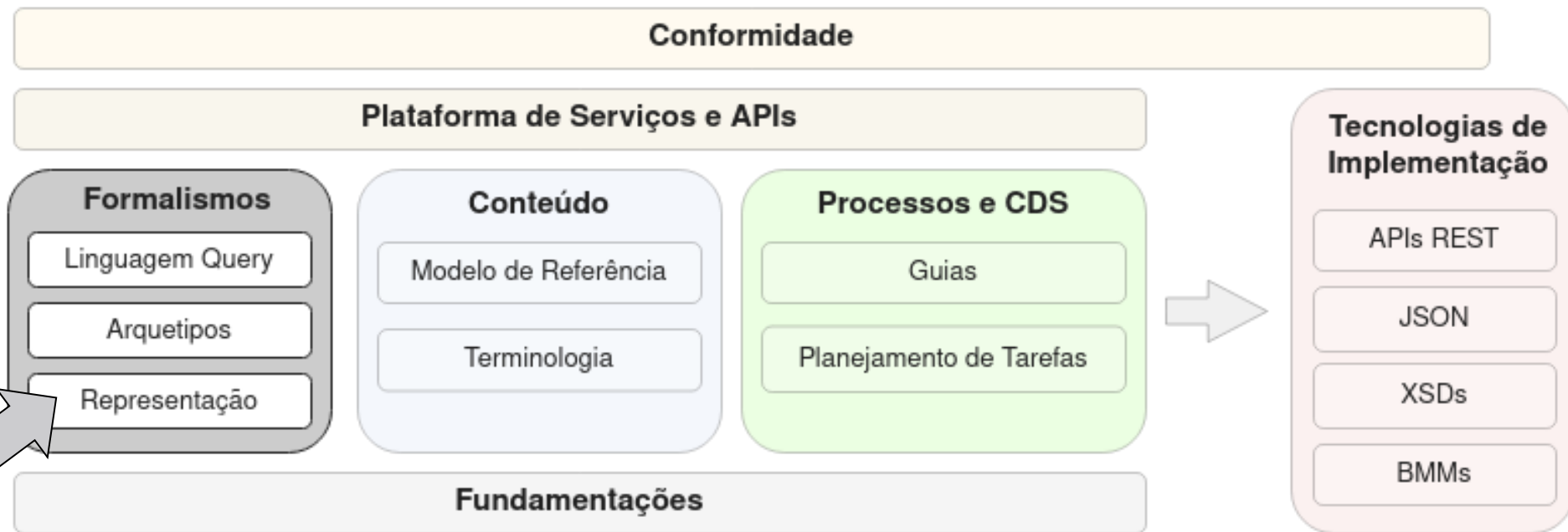
Modelo de Referência Genérico

openEHR



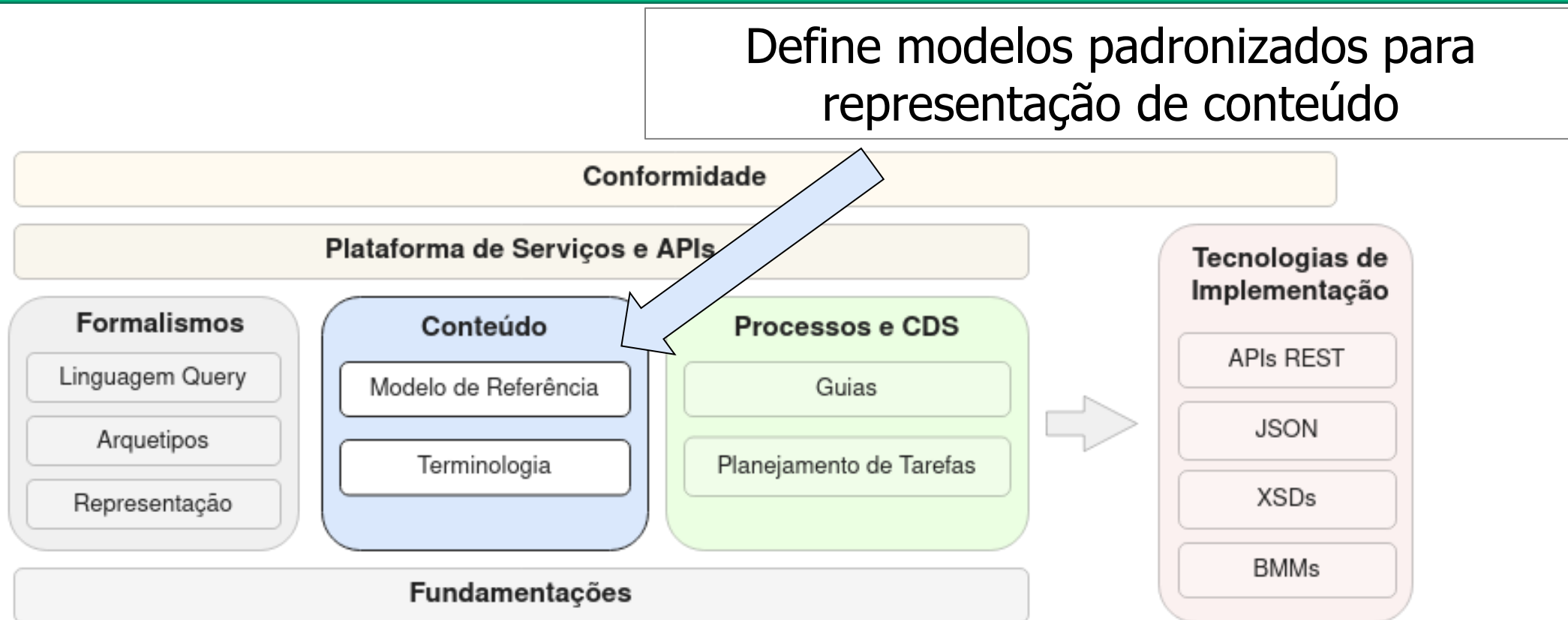
Biblioteca de classes de contexto médico de finalidade pré-definida (classes para médicos, pacientes, medicamentos, procedimentos etc.)

Modelo de Referência Genérico openEHR



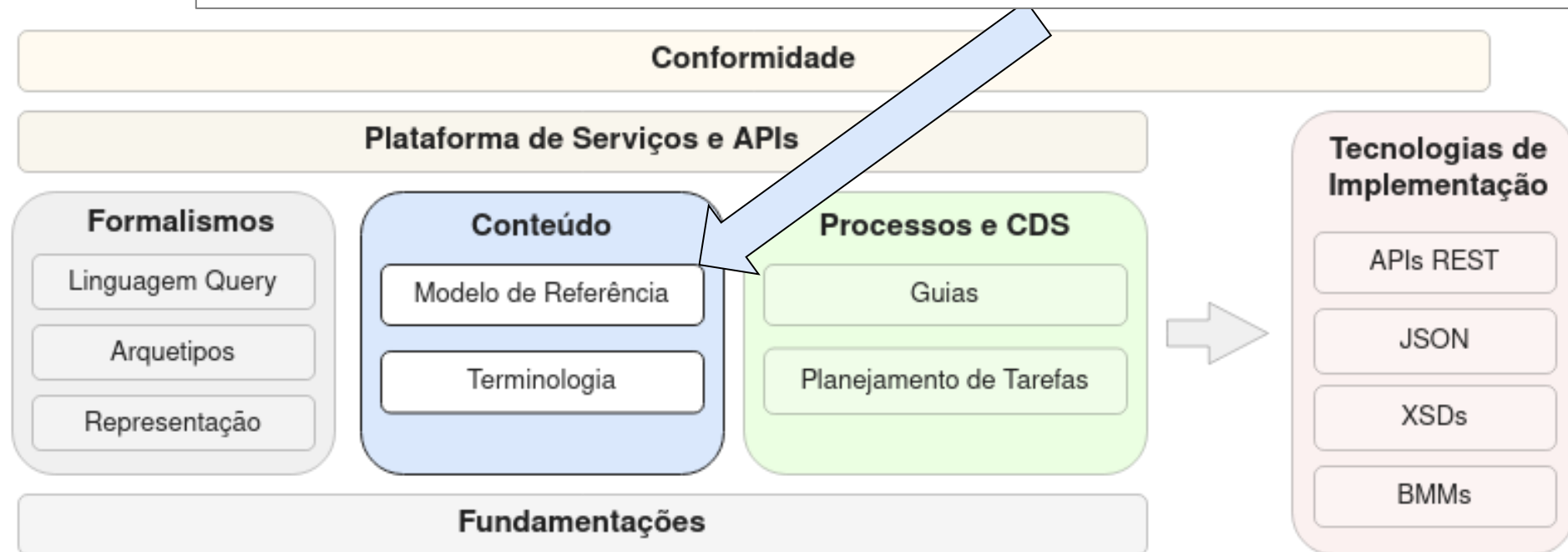
Coleção da representação das classes internas e dos arquétipos utilizando UML

Modelo de Referência Genérico openEHR

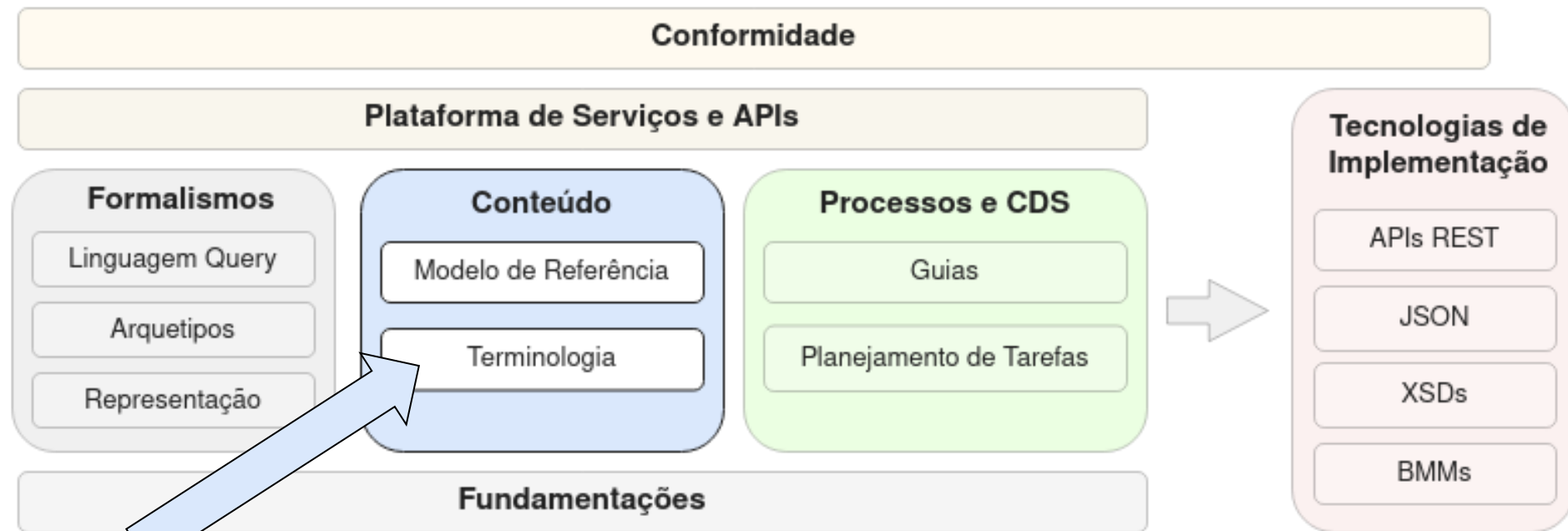


Modelo de Referência Genérico openEHR

Definição do componente de conteúdo primário, como dados demográficos dos pacientes e registro médicos eletrônicos



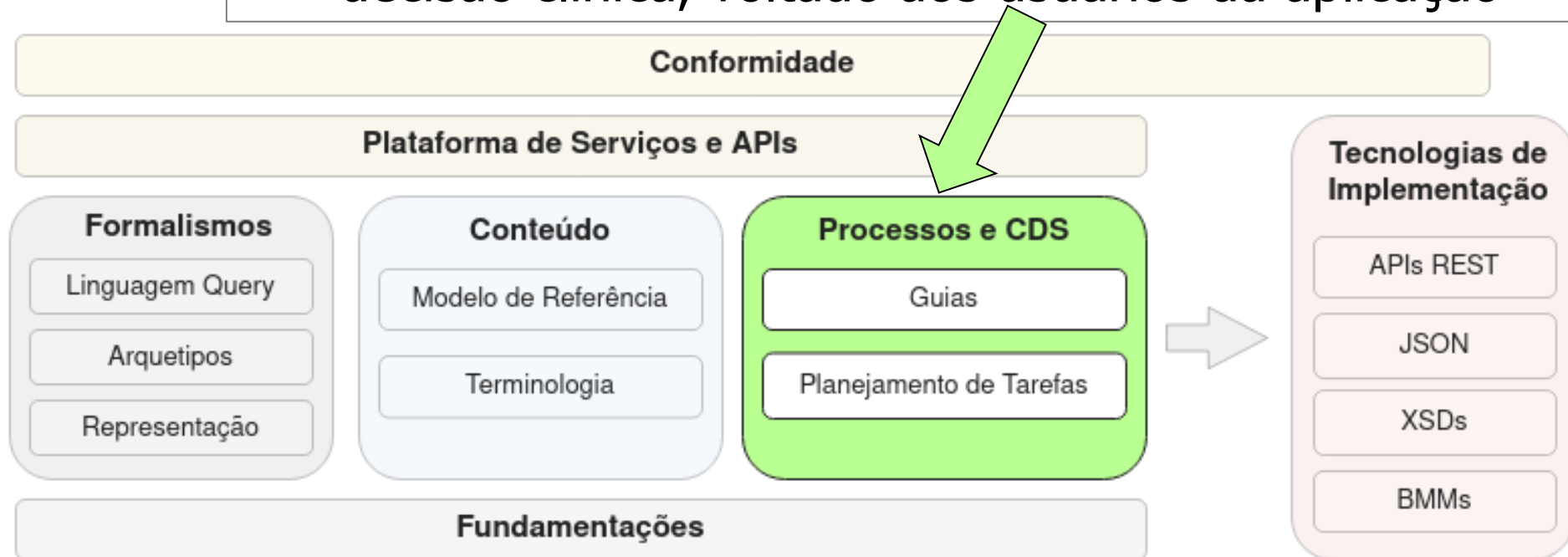
Modelo de Referência Genérico openEHR



Suporte para integração dos dados dos sistemas aos vocabulários de terminologias padronizadas

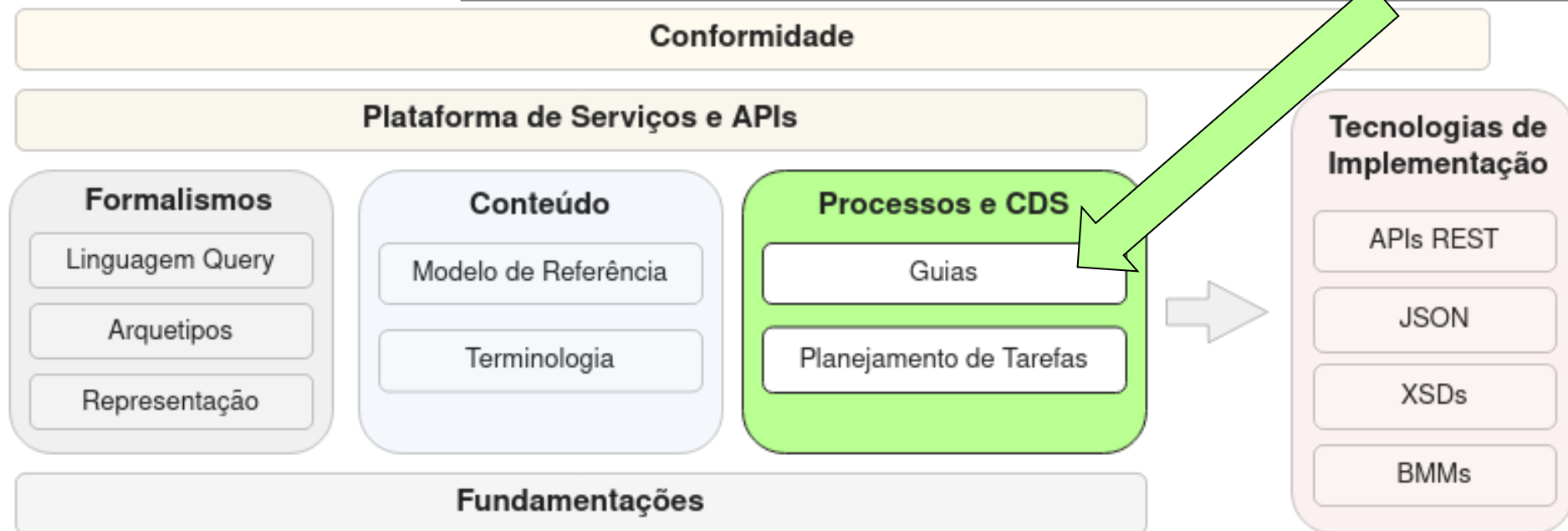
Modelo de Referência Genérico openEHR

Define componentes do processo clínico e do suporte à decisão clínica, voltado aos usuários da aplicação

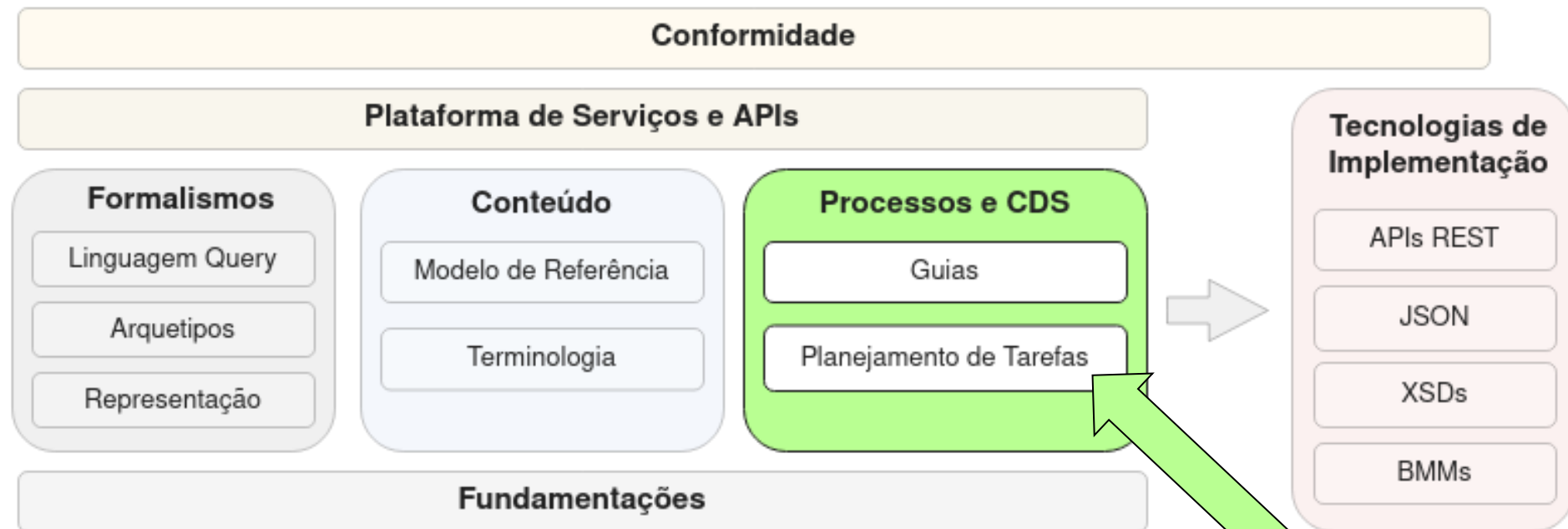


Modelo de Referência Genérico openEHR

Suporte para a documentação e produção do manual do sistema desenvolvido sobre o openEHR

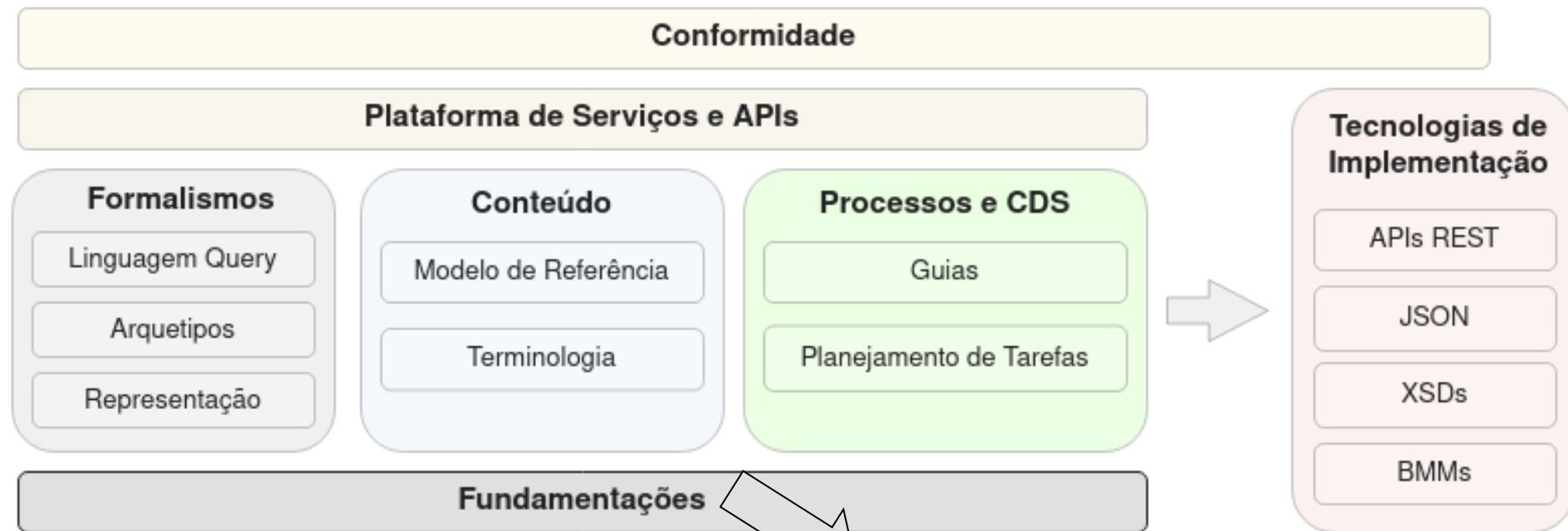


Modelo de Referência Genérico openEHR



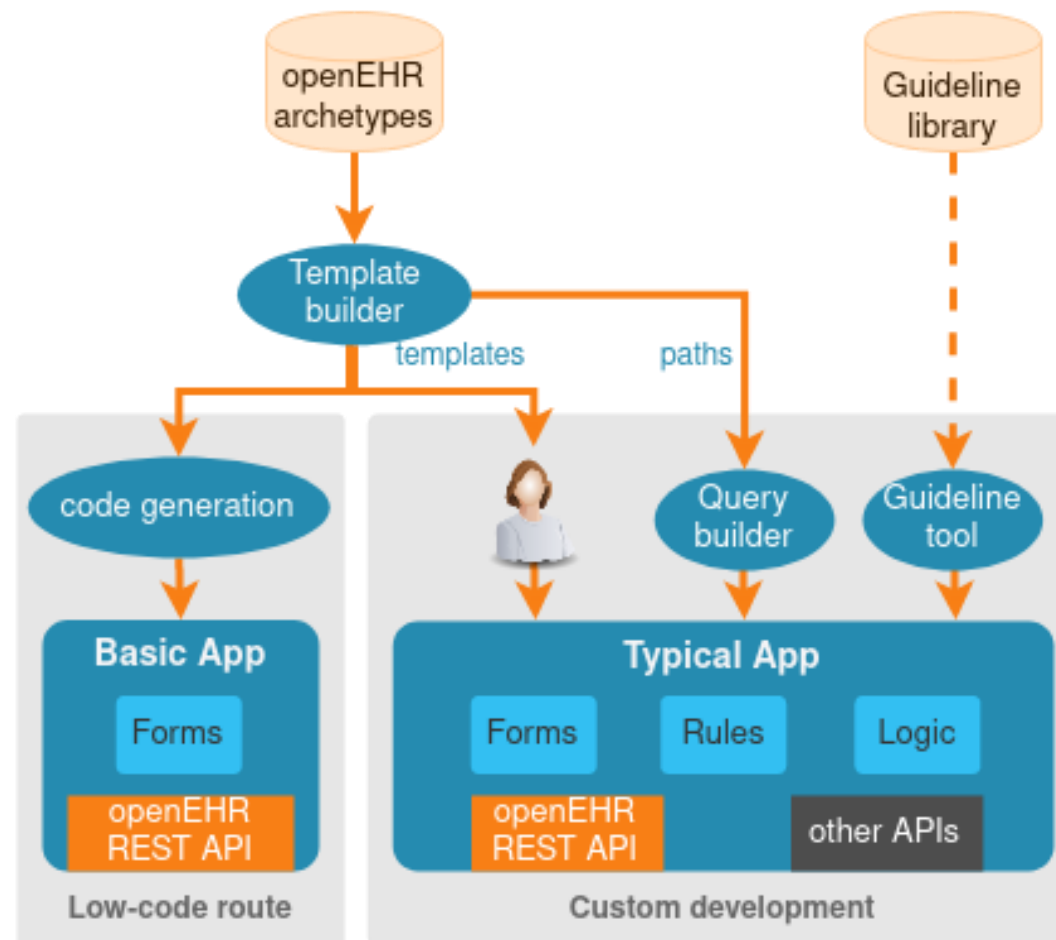
Manual de uso da aplicação organizado por situação clínica ou tarefas de contexto médico

Modelo de Referência Genérico openEHR

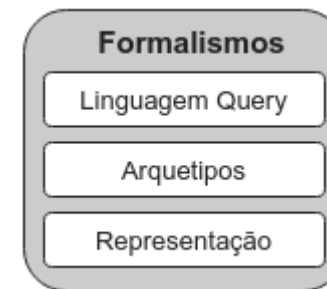
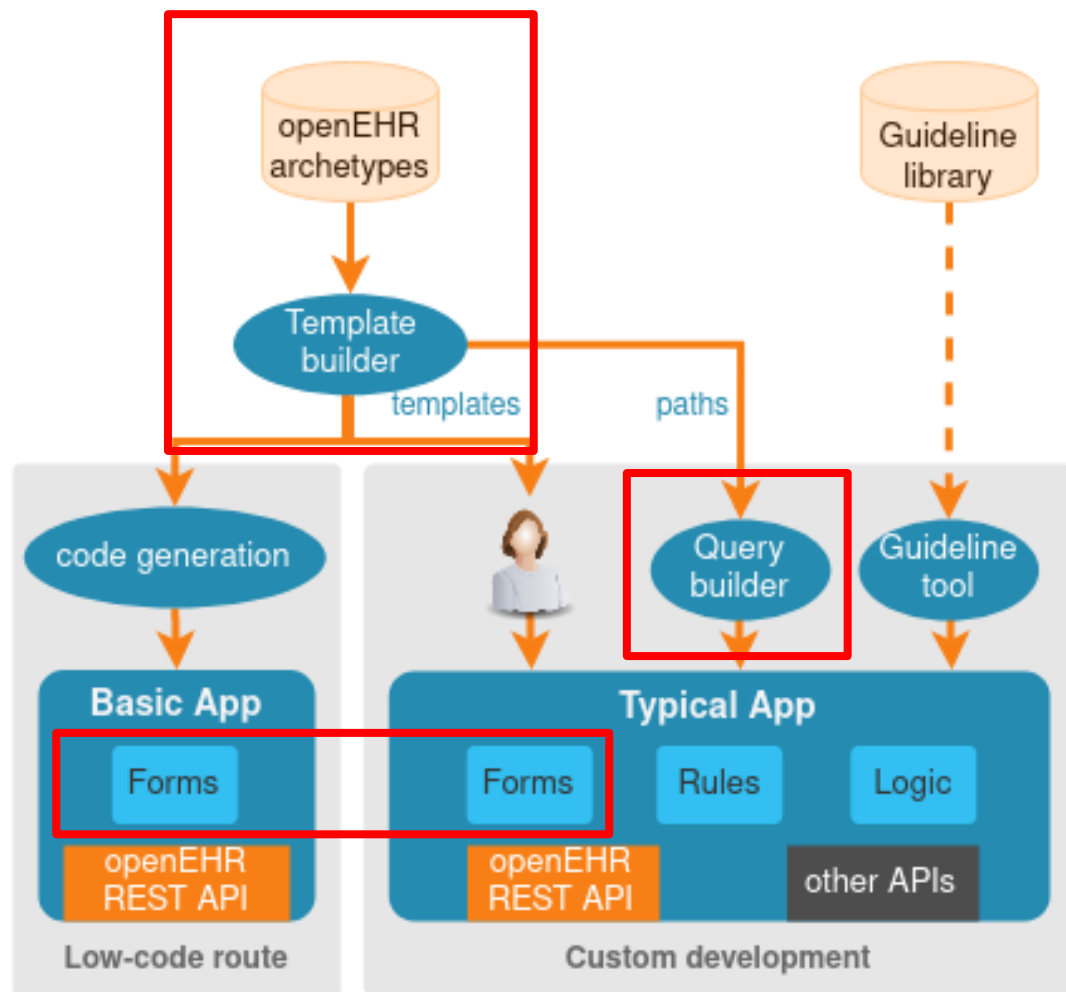


Define classes fundamentais para o funcionamento do sistema baseado em openEHR, como tipos primitivos de dados

Arquitetura openEHR para Aplicações Médicas

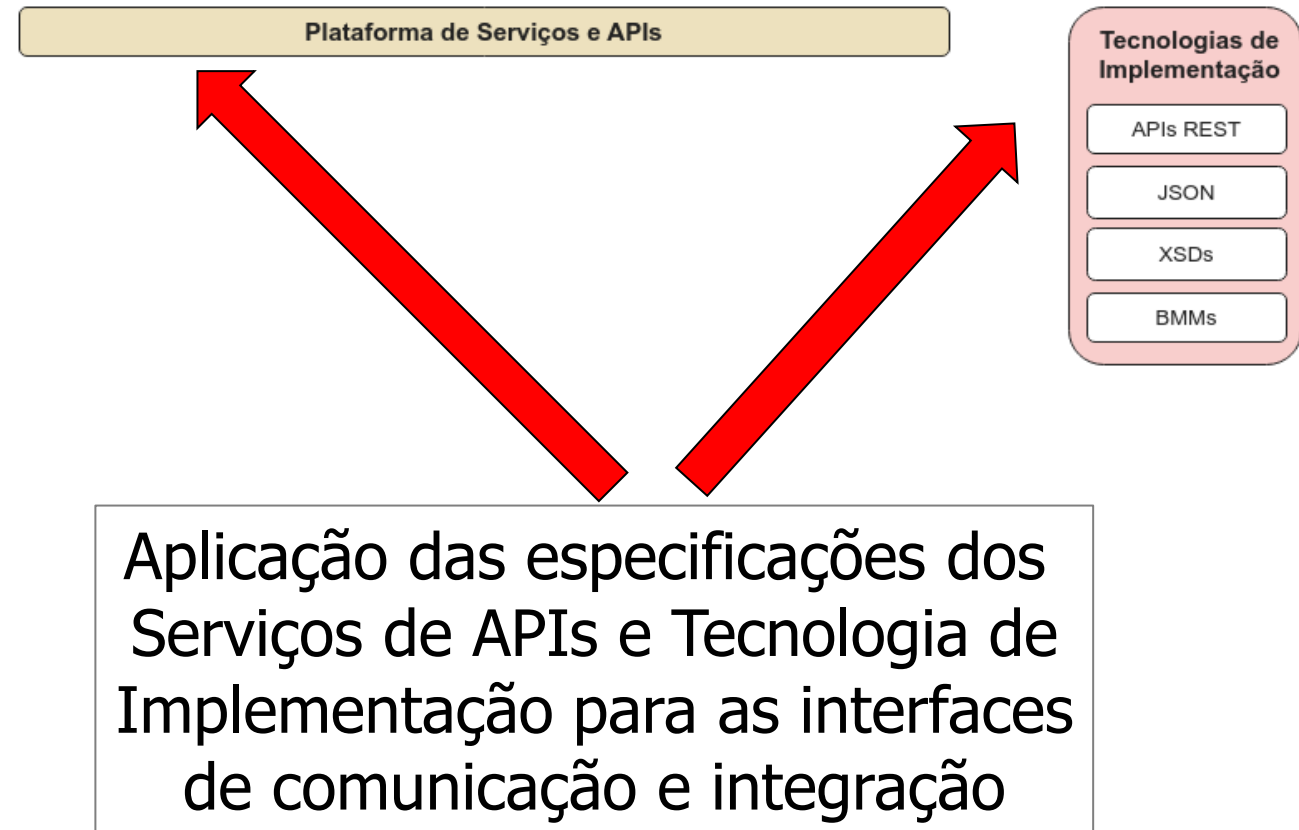
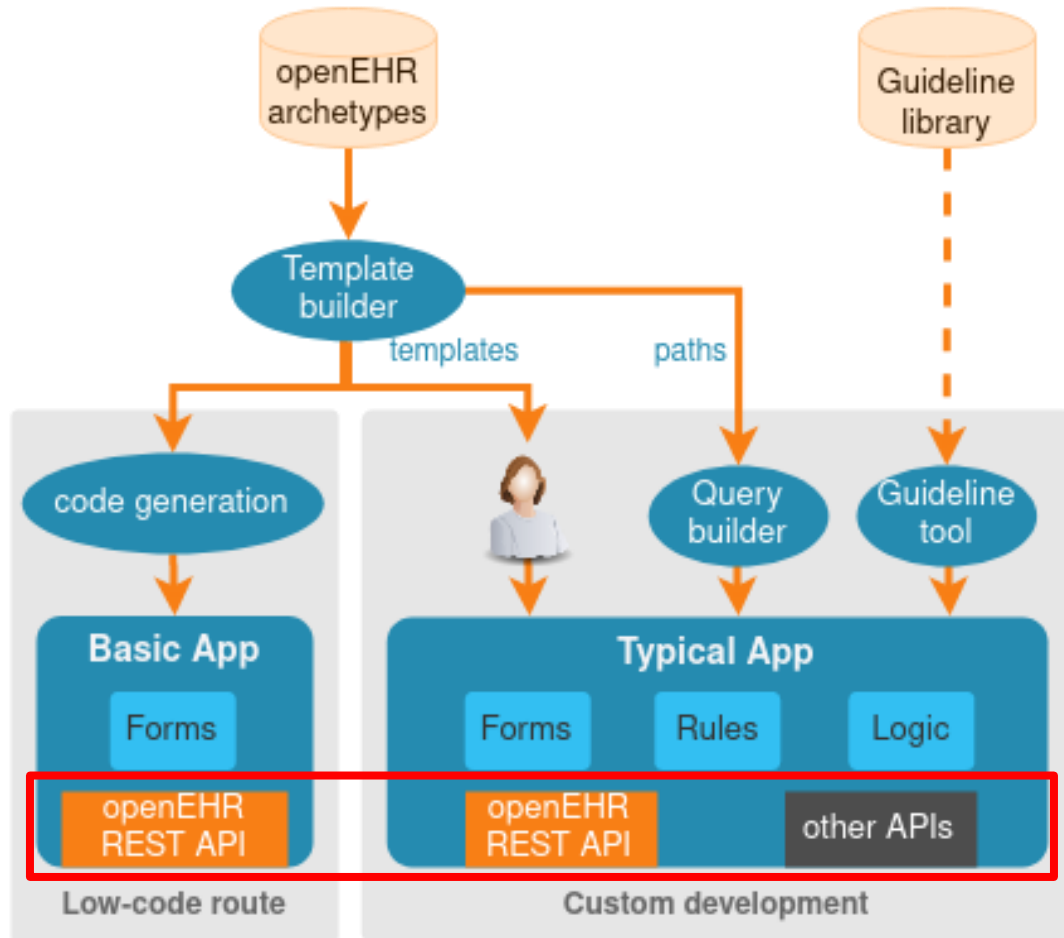


Arquitetura openEHR para Aplicações Médicas

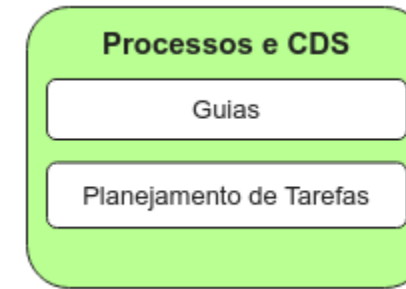
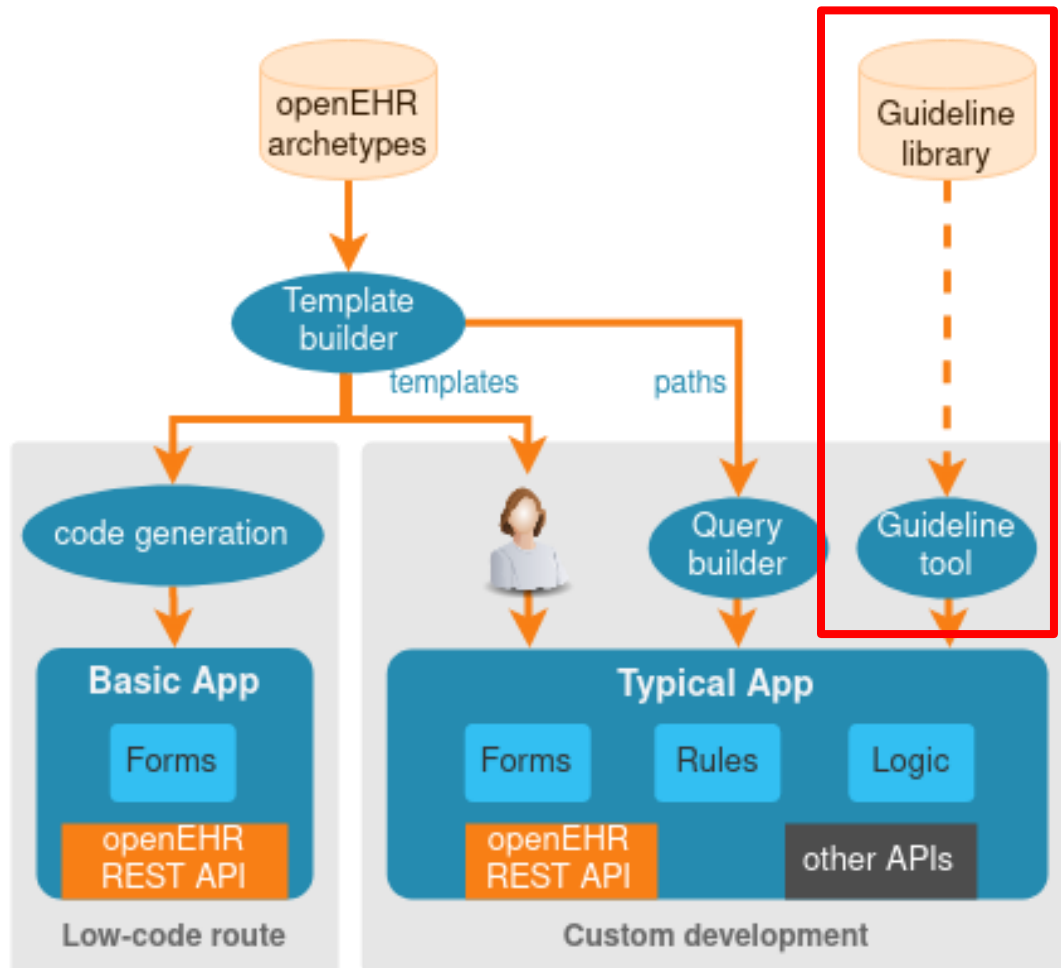


Aplicação das especificações dos componentes de Formalismos para entrada e leitura de dados

Arquitetura openEHR para Aplicações Médicas

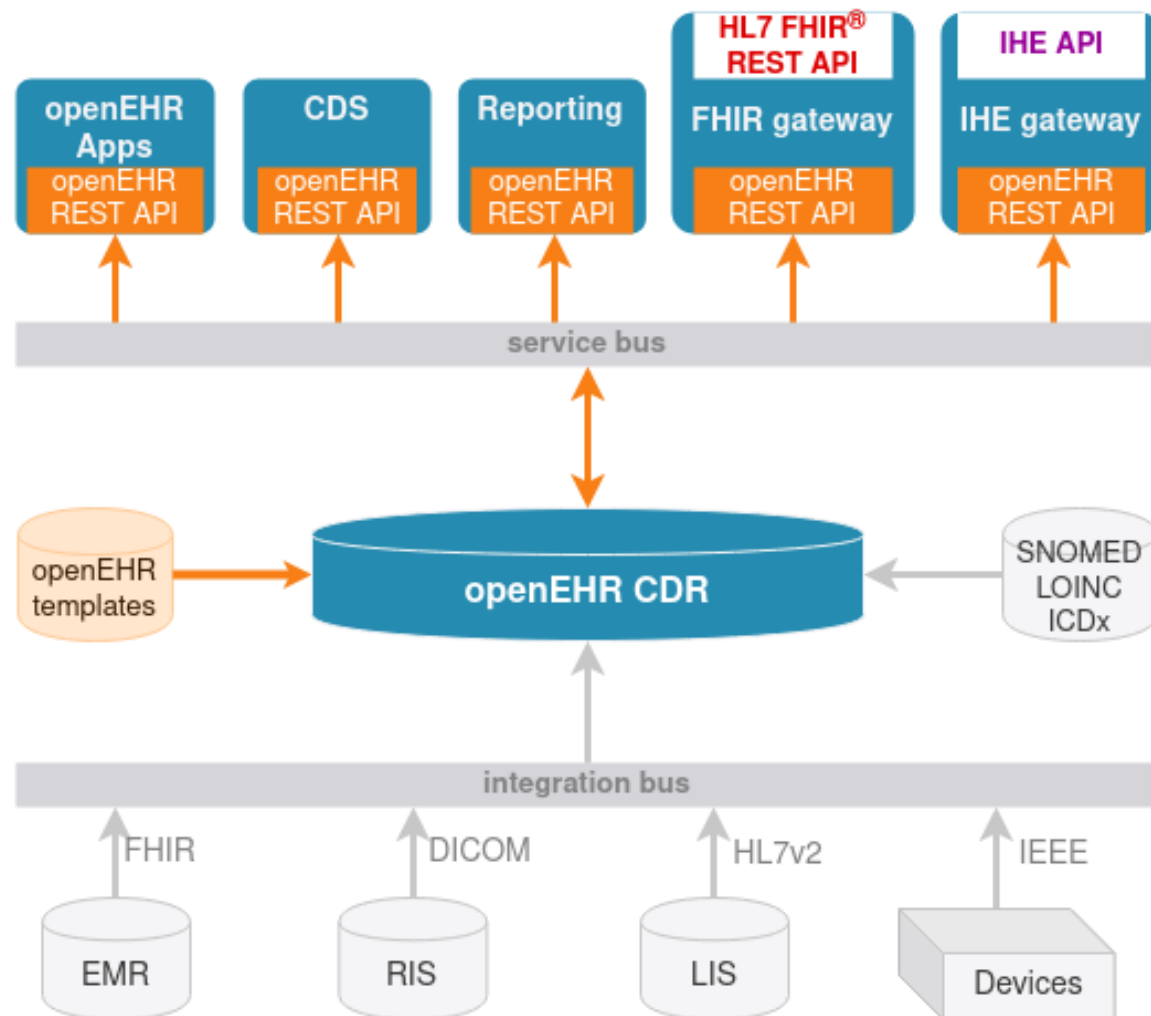


Arquitetura openEHR para Aplicações Médicas

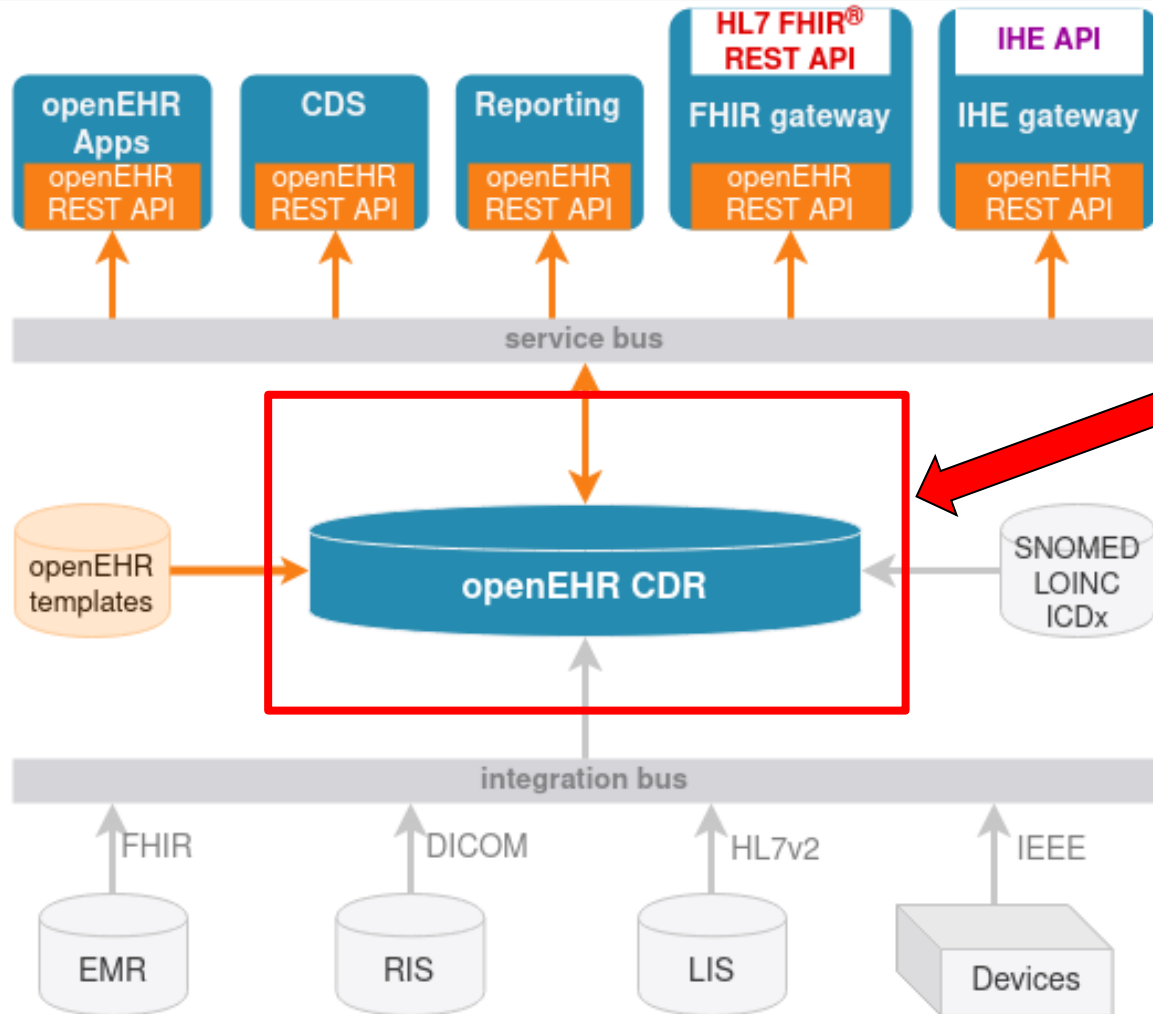


Aplicação das especificações dos Processos e CDS para o desenvolvimento do manual de uso do software

Arquitetura openEHR para Integração de Sistemas



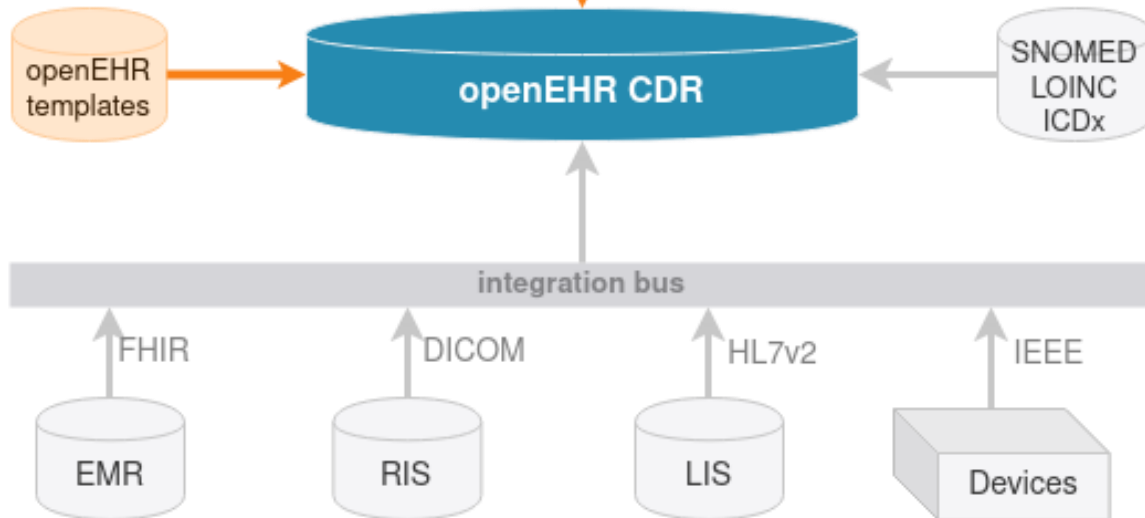
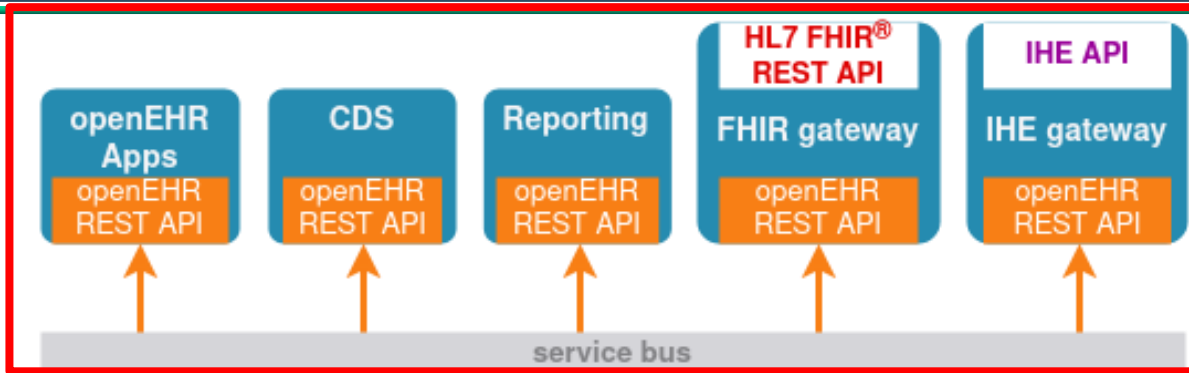
Arquitetura openEHR para Integração de Sistemas



Integração de múltiplos sistemas por meio de uma base de dados padronizada e compartilhada

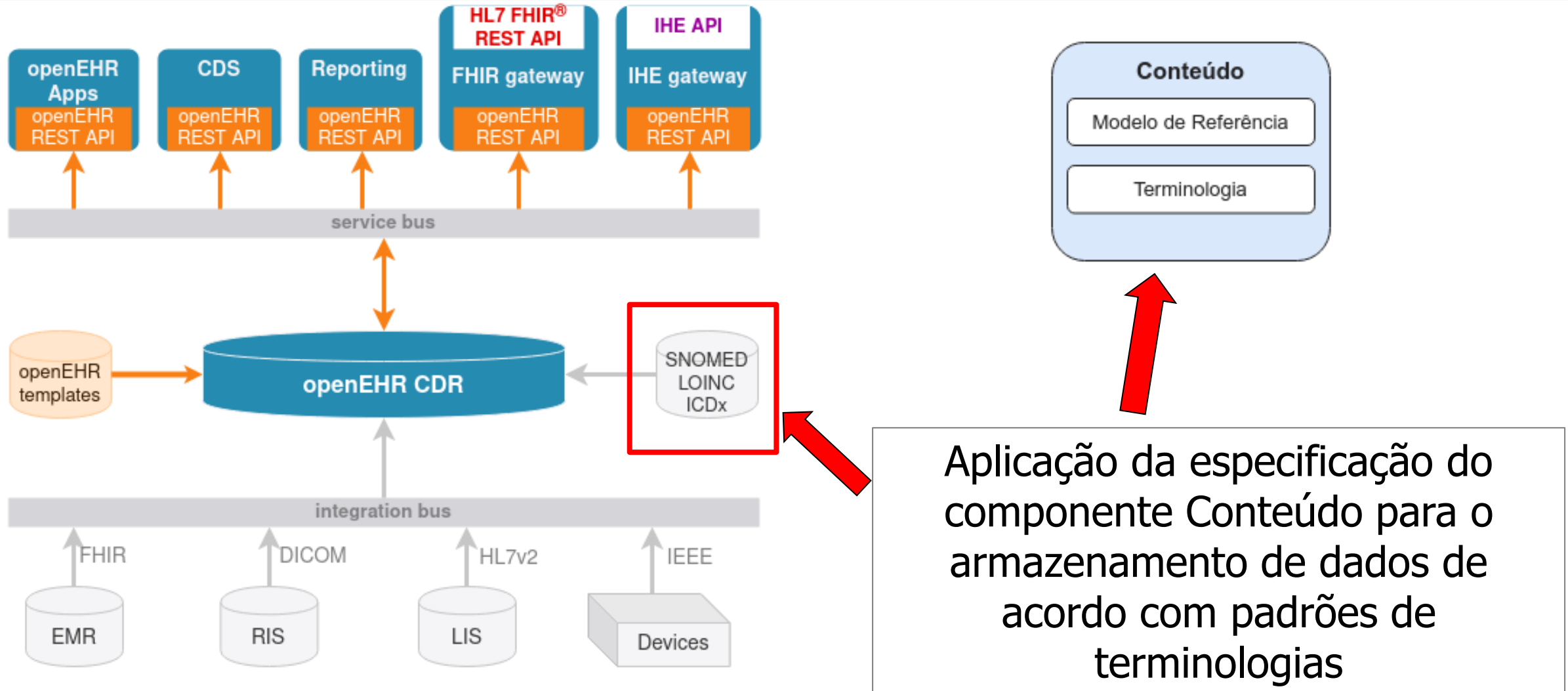
CDR (Clinical Data Repository)

Arquitetura openEHR para Integração de Sistemas

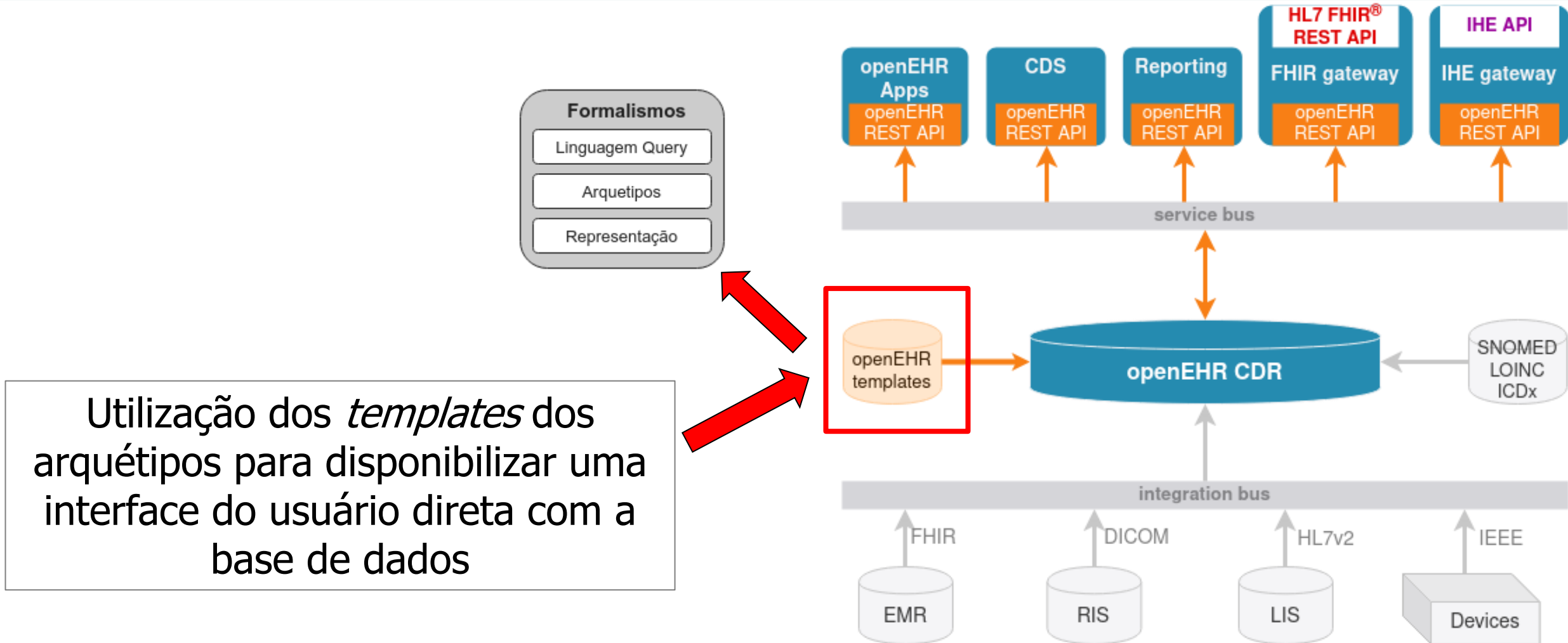


Integração com os serviços e aplicações openEHR naturalmente suportados, ampliando as funcionalidades dos softwares integrados

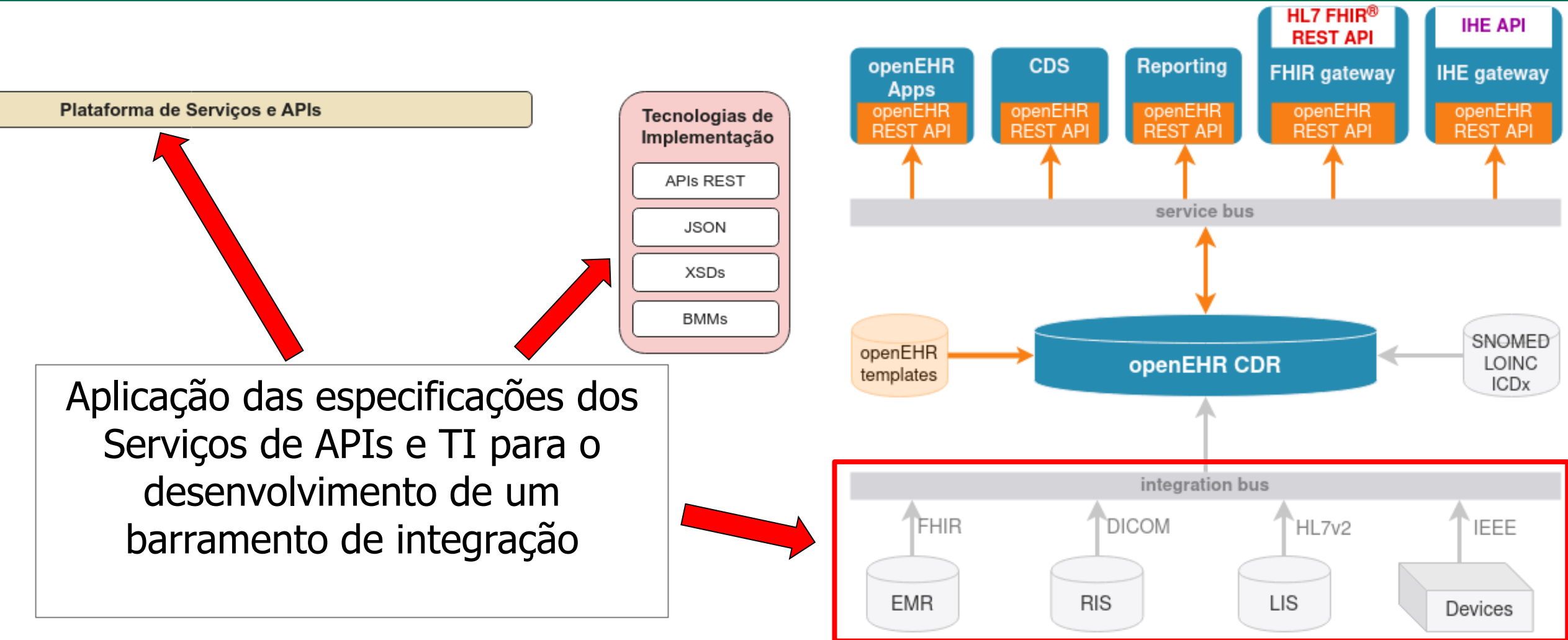
Arquitetura openEHR para Integração de Sistemas



Arquitetura openEHR para Integração de Sistemas



Arquitetura openEHR para Integração de Sistemas



Aplicação das especificações dos Serviços de APIs e TI para o desenvolvimento de um barramento de integração

- Especificação da estrutura dos documentos eletrônicos e dos tipos de dados que os documentos devem ter
- Atribuição de semântica aos documentos que ajudam no tratamento continuado dos pacientes
 - Geração de histórico
 - Armazenamento de informações úteis

- Especificado e mantido pela Health Level 7 (HL7)
 - Uma das maiores organizações padronizadoras para aplicações de saúde
- Representa os dados dos registros médicos em formato XML
- Especificado e organizado para casos de uso (*template*)
 - Torna-se menos genérico pelo uso de *templates*
 - Possui 12 documentos distintos de especificação




```
<section>
  <templateId root="2.16.840.1.113883.10.20.22.2.6.1"/>
  <templateId root="2.16.840.1.113883.10.20.22.2.6.1" extension="2015-08-01"/>
  <!-- Allergies (entries required) section template -->
  <code code="48765-2" codeSystem="2.16.840.1.113883.6.1"/>
  <title>Allergies, Adverse Reactions and Alerts</title>
  <text><content ID="allergyobs1">Not Allergic to Peanuts</content></text>
  <!-- Could include two tables with one recording active allergies and another with Not Allergic - Need to clearly denote-->
  <entry typeCode="DRIV">
    <act classCode="ACT" moodCode="EVN">
      <!-- ** Allergy problem act ** -->
      <templateId root="2.16.840.1.113883.10.20.22.4.30"/>
      <templateId root="2.16.840.1.113883.10.20.22.4.30" extension="2015-08-01"/>
      <id root="91a4e6a1-e192-438c-a85d-abb210af6d25"/>
      <code code="CONC" codeSystem="2.16.840.1.113883.5.6"/>
      <text>
        <reference value="#allergyobs1"/>
      </text>
      <statusCode code="active"/>
      <!-- This is the time stamp for when the non-allergy was first documented as a concern-->
      <effectiveTime>
        <low value="20140104123506-0500"/>
      </effectiveTime>
    </act>
  </entry>

```

Registro de informação de paciente: "não é alérgico a uma substância específica" (ex.: amendoim)

Estrutura definida pela especificação do XML no modelo CDA

```
<section>
  <templateId root="2.16.840.1.113883.10.20.22.2.6.1"/>
  <templateId root="2.16.840.1.113883.10.20.22.2.6.1" extension="2015-08-01"/>
  <!-- Allergies (entries required) section template -->
  <code code="48765-2" codeSystem="2.16.840.1.113883.6.1"/>
  <title>Allergies, Adverse Reactions and Alerts</title>
  <text><content ID="allergyobs1">Not Allergic to Peanuts</content></text>
  <!-- Could include two tables with one recording active allergies and another with Not Allergic - Need to clearly denote-->
  <entry typeCode="DRIV">
    <act classCode="ACT" moodCode="EVN">
      <!-- ** Allergy problem act ** -->
      <templateId root="2.16.840.1.113883.10.20.22.4.30"/>
      <templateId root="2.16.840.1.113883.10.20.22.4.30" extension="2015-08-01"/>
      <id root="91a4e6a1-e192-438c-a85d-abb210af6d25"/>
      <code code="CONC" codeSystem="2.16.840.1.113883.5.6"/>
      <text>
        <reference value="#allergyobs1"/>
      </text>
      <statusCode code="active"/>
      <!-- This is the time stamp for when the non-allergy was first doc
      <effectiveTime>
        <low value="20140104123506-0500"/>
      </effectiveTime>
    </act>
  </entry>

```

Conteúdo definido pela especificação do contexto do *template* e identificado por um valor numérico único

Pode usar códigos de terminologias específicas

- Especificado e mantido pela Health Level 7 (HL7)
- Representação de registros médicos em formato XML, JSON ou RDF
- Especificação de documentos em formato próprio (Recurso)
 - Metadados e identificadores
 - Resumo humanamente legível
 - URL para a definição do Recurso
 - Dados do registro médico eletrônico



```
<id value="glossy"/>  
<meta>  
  <lastUpdated value="2014-11-13T11:41:004 11:00"/>  
</meta>
```

**Metadados &
Identificação**

```
<text>  
  <status value="generated"/>  
  <div xmlns="http://www.v3.org/1999/xhtml">  
    <p>Henry Levin the 7th</p>  
    <p>MRN:123456. Male, 24-Sept 1932</p>  
  </div>  
</text>
```

**Resumo
Humanamente
Legível**

```
<extension url="http://example.org/StructureDefinition/triais">  
  <valueCode value="renal"/>  
</extension>
```

**Extensão com
URL para
definição**

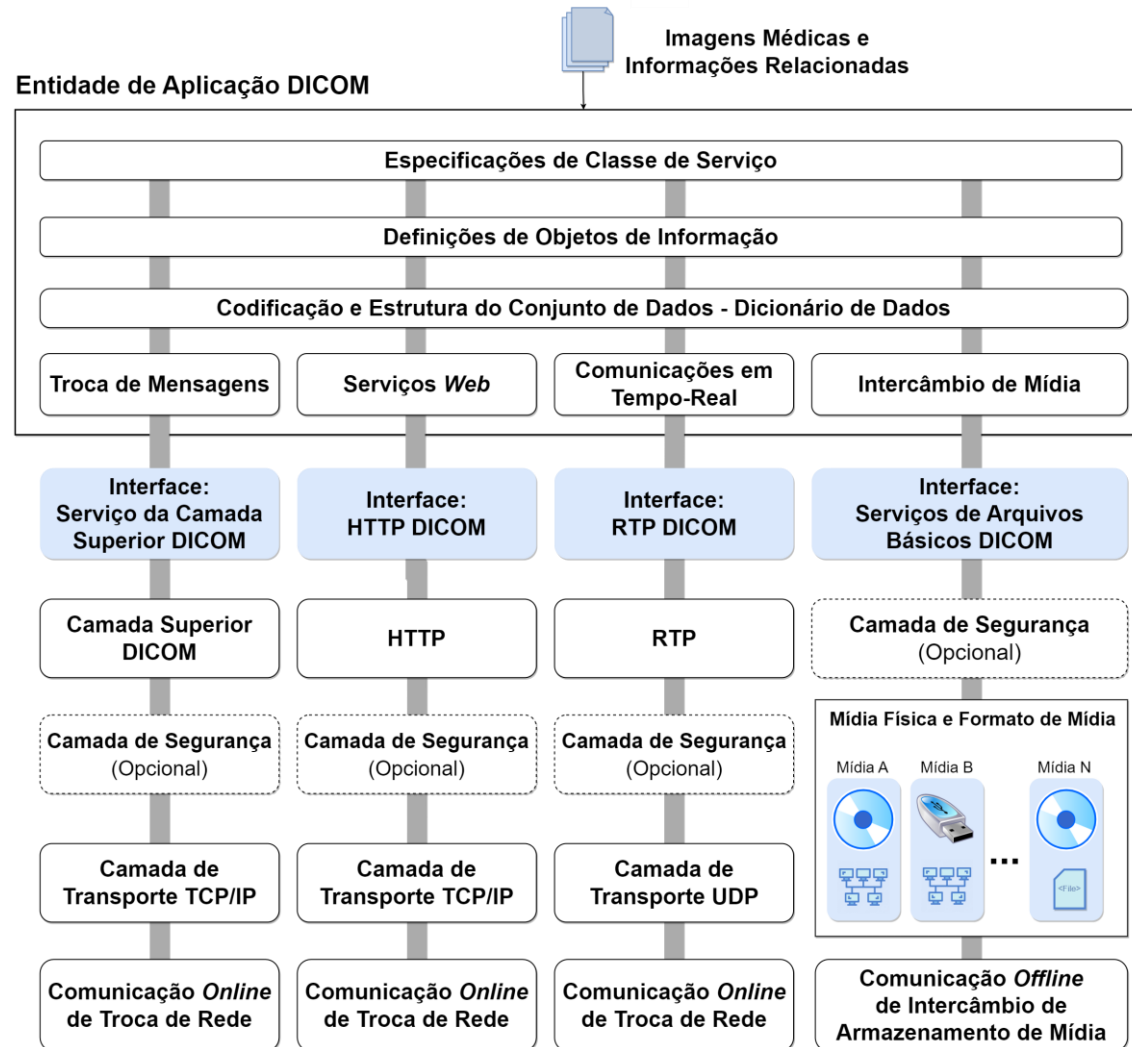
```
<identifier>
  <use value="usual"/>
  <type>
    <coding>
      <system value="http://hl7.org/fhir/v2/0203"/>
      <code value="MR"/>
    </coding>
  </type>
  <system value="http://www.goodhealth.org/identifiers/mrn"/>
  <value value="123456"/>
</identifier>
<active value="true"/>
<name>
  <family value="Levin"/>
  <given value="Henry"/>
  <suffix value="The 7th"/>
</name>
<gender value="male"/>
<birthDate value="1932-09-24"/>
<careProvider>
  <reference value="Organization/2"/>
  <display value="Good Health Clinic"/>
</careProvider>
```

Dados Padronizados:

- MRN (*Medical Record Number*)
- Nome
- Gênero
- Data de Nascimento
- Plano de Saúde

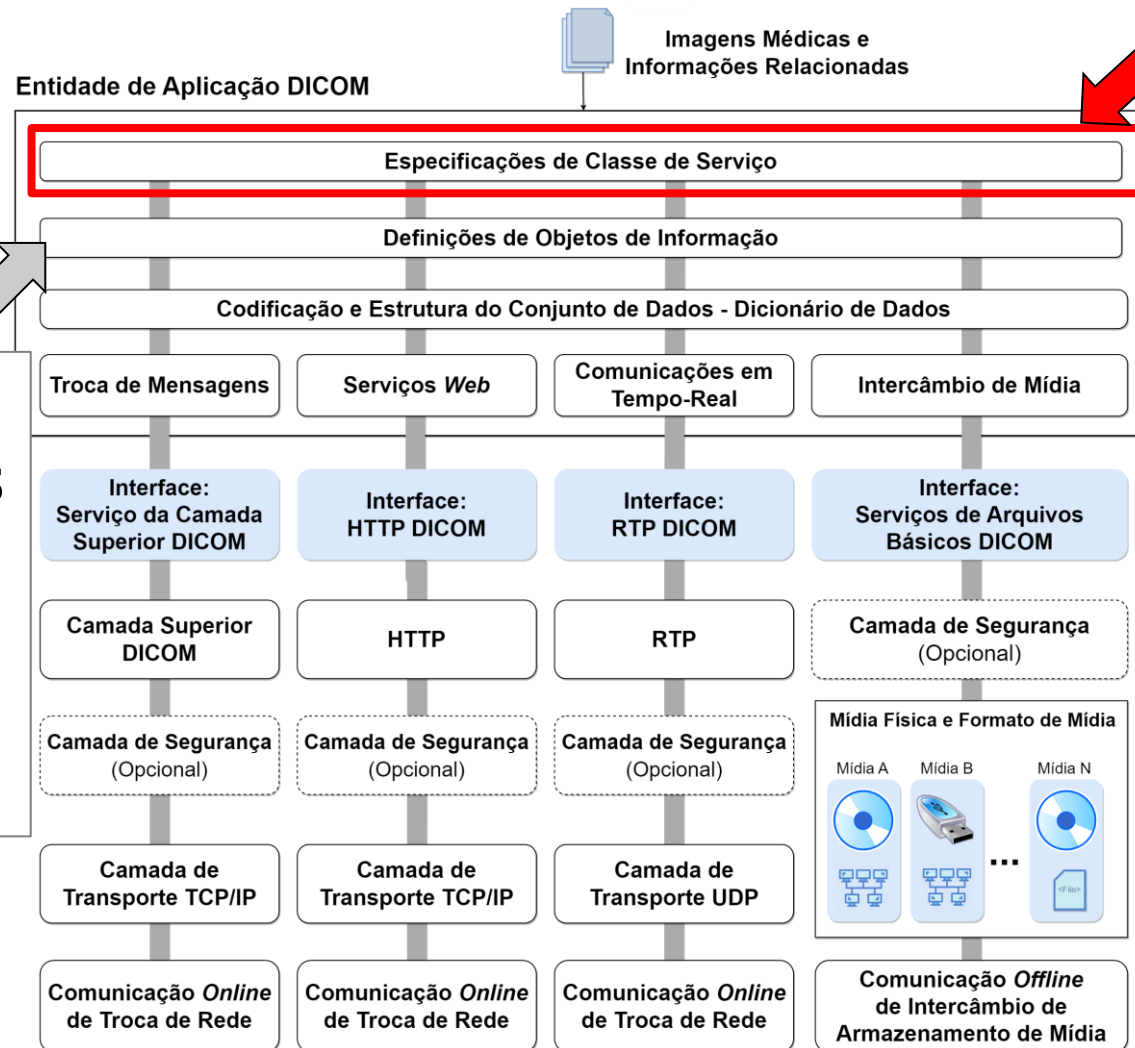
- Padrão internacional focado em especificações para imagens médicas
 - Tomografia computadorizada, ressonância magnética, radiografia e outros exames de imagem
- Definição de serviços auxiliares para análise das imagens
 - Formato de arquivo e armazenamento
- Adição de informações para auxílio ao diagnóstico
 - Dados demográficos
 - Parâmetros de aquisição para o estudo de imagem
 - Dimensões da imagem e espaço de cores

Modelo Geral dos Serviços DICOM



Define uma arquitetura que vai além da representação da imagem

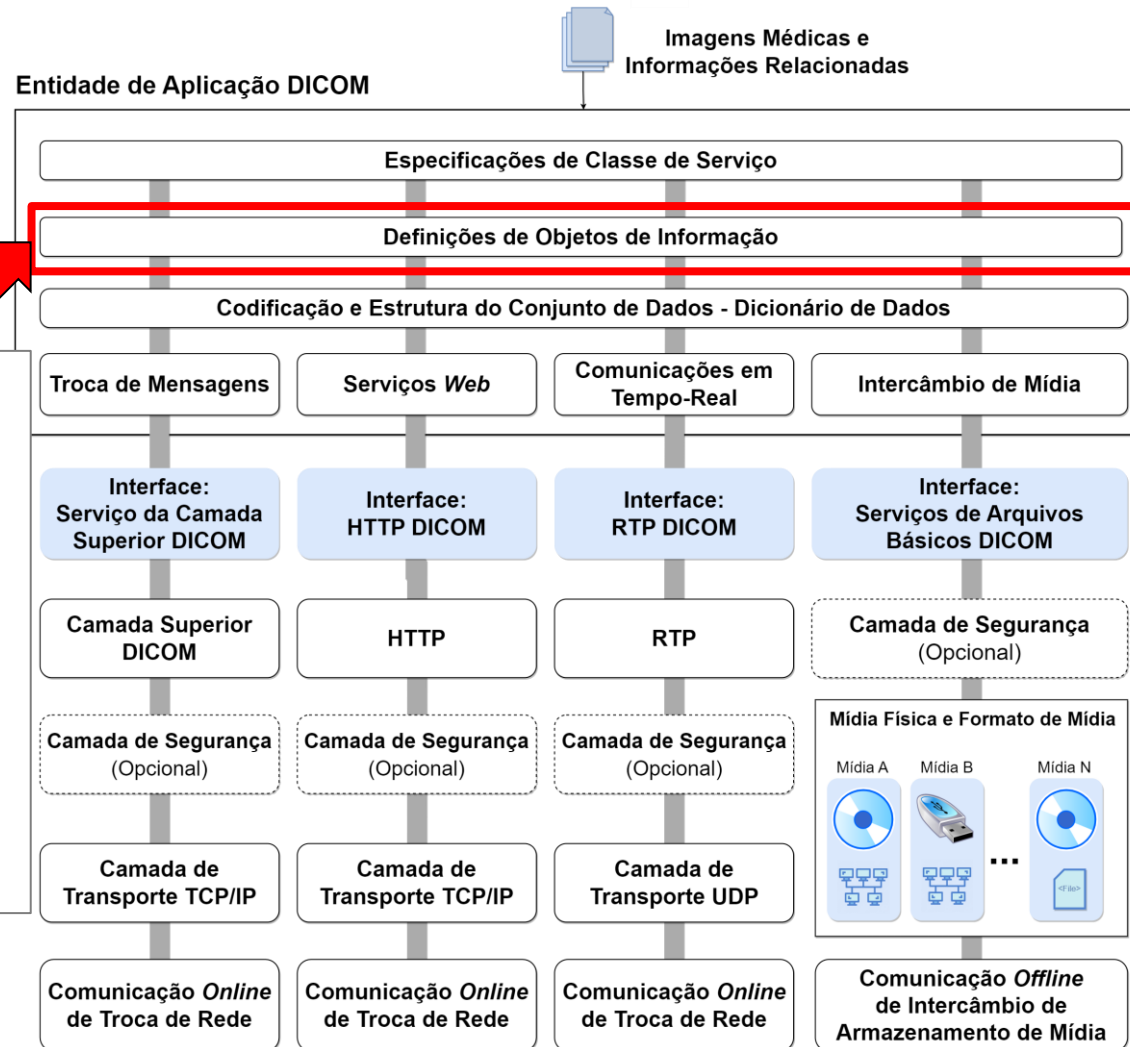
Modelo Geral dos Serviços DICOM



Classes de Serviço operam sobre objetos de informação por meio de comandos específicos para cada serviço

Classes dos serviços especificados pelo DICOM (Ex.: Classe de Serviço de Armazenamento, Classe de Serviço de Query/Busca etc.)

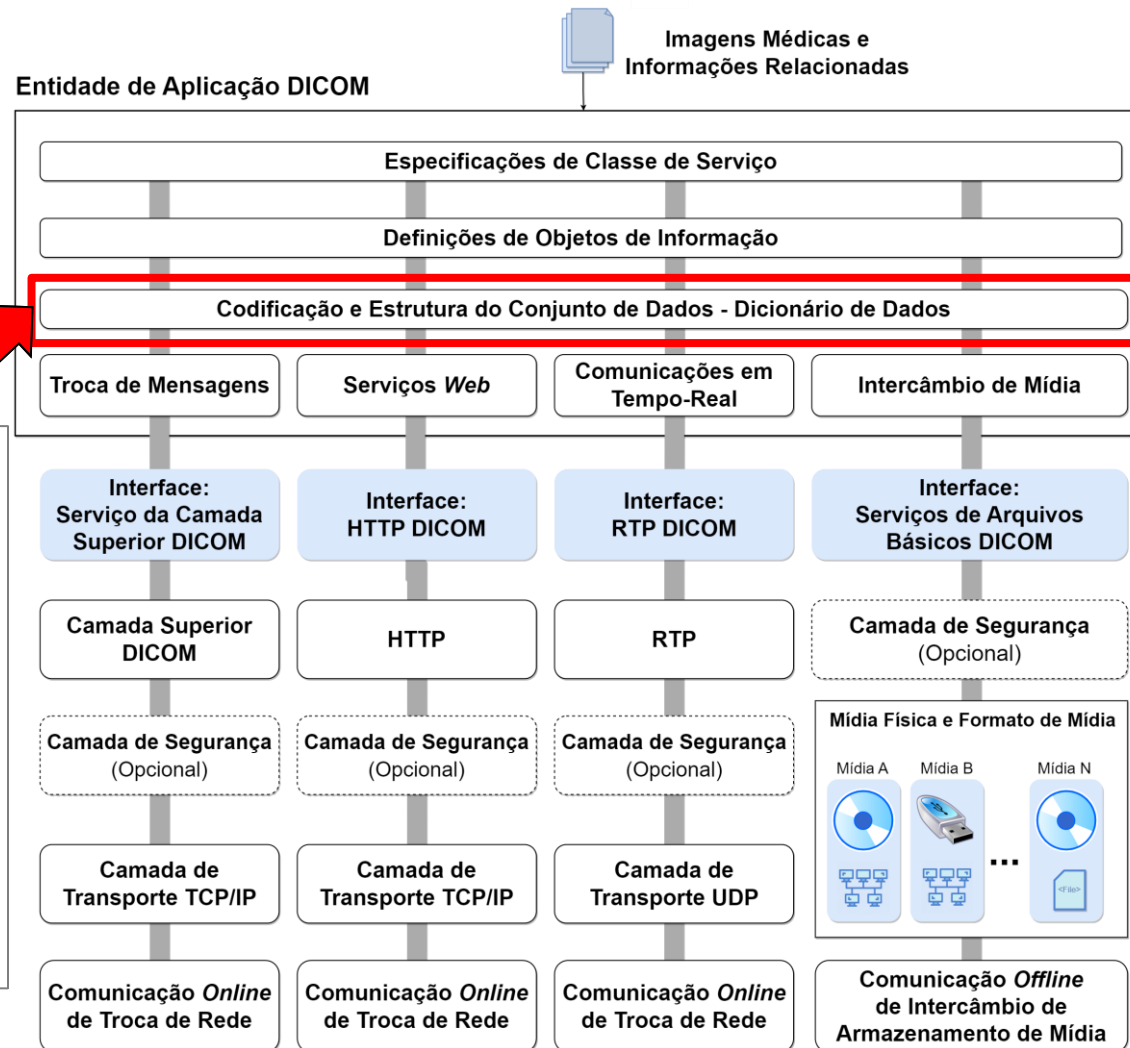
Modelo Geral dos Serviços DICOM



Informações sobre características físicas envolvidas na coleta da imagem (Ex.: formas de onda, relatórios estruturados, dose de radioterapia etc.)

Pode conter dados demográficos do paciente

Modelo Geral dos Serviços DICOM

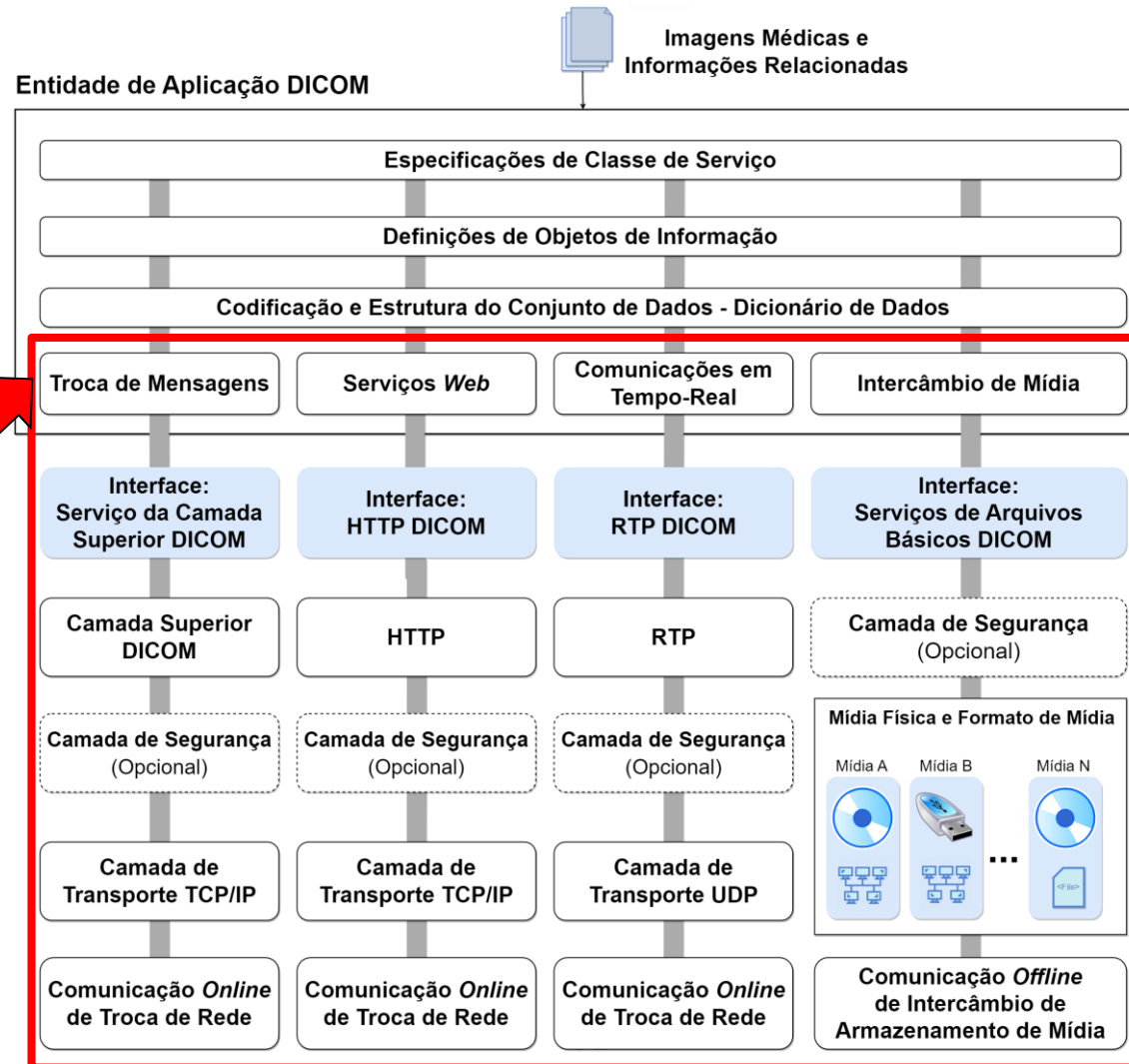


Mantém a referência para especificação DICOM dos arquivos

Responsável por todas as operações sobre os arquivos de imagem (Ex: codificação, conversão e disponibilização para consumo)

Controla a indexação dos arquivos, dando nome, organizando em grupos de acordo com as características e adicionando identificadores únicos

Modelo Geral dos Serviços DICOM



Comunicação

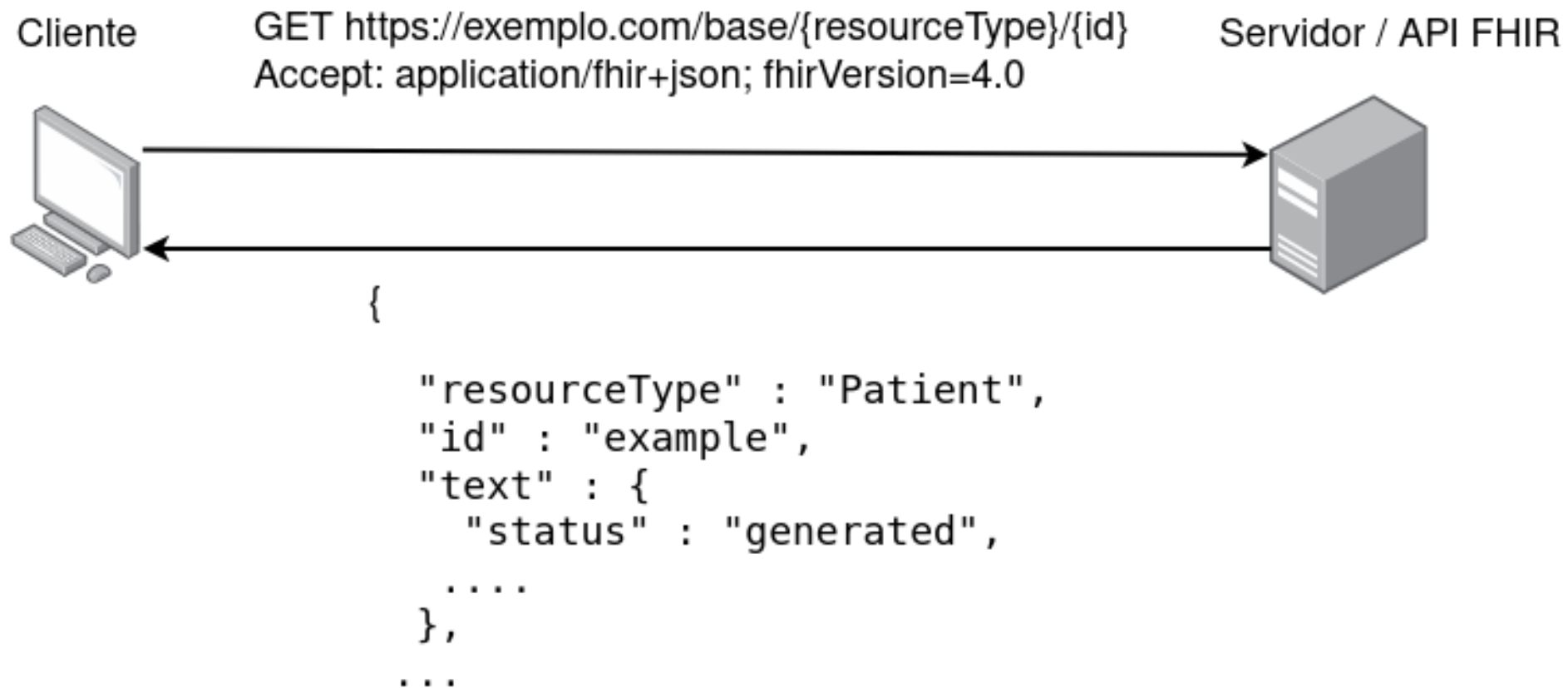
- **Objetivos**

- Definir padrão de transferência de dados entre sistemas de saúde distintos
- Promover a **interoperabilidade** entre sistemas de saúde
- Definir sintaxe, semântica e o fluxo de dados das mensagens dos sistemas de saúde

- Aproveita as convenções de comunicação *web* já consolidadas
 - Troca de dados através de APIs RESTful baseadas em HTTP
- Suporta sistemas com arquitetura orientada a serviço
 - Tendências da nova geração dos *softwares*
 - Permite operações unitárias ou em lote
- Baseado no paradigma CRUD para interagir com os serviços
 - Além de dar suporte para chamadas de execução de processos remotos

Read Request – FHIR

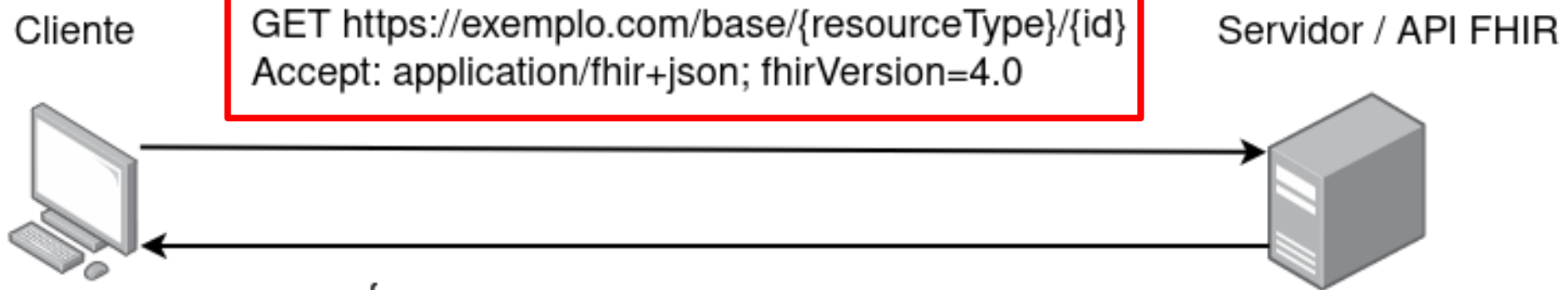
Exemplo



Read Request – FHIR

Exemplo

Requisição HTTP para leitura com especificação do formato de retorno no cabeçalho



```
{
```

```
  "resourceType" : "Patient",
  "id" : "example",
  "text" : {
    "status" : "generated",
```

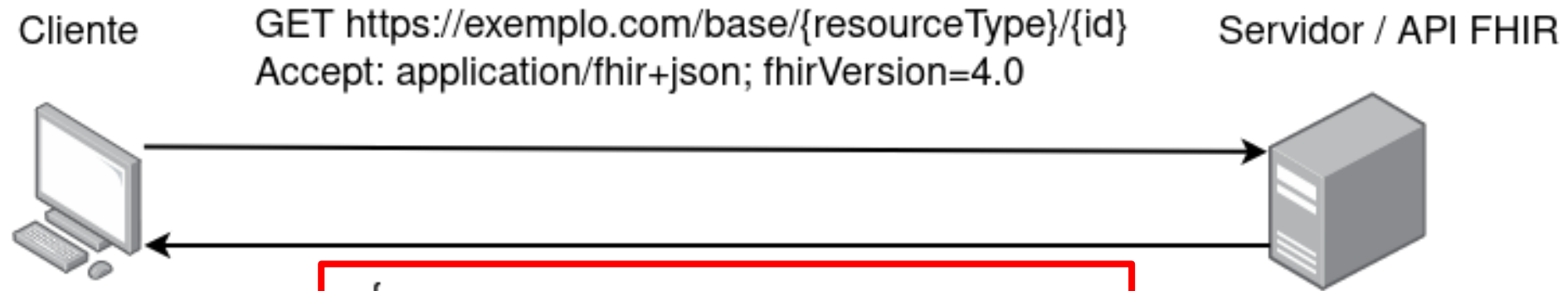
```
    ....
```

```
  },
```

```
  ...
```

Read Request – FHIR

Exemplo



```
{
  "resourceType" : "Patient",
  "id" : "example",
  "text" : {
    "status" : "generated",
    ....
  },
  ...
}
```

Recurso FHIR no formato e versão especificados na requisição

- Define o conteúdo e corpo das mensagens
 - Conteúdo depende do tipo específico da requisição
- Especifica os tipos de requisição baseadas no contexto de situações médicas
 - Dados demográficos, histórico de consultas, histórico imunológico etc.
 - Cada requisição deve seguir os passos de uma máquina de estados para garantir o envio e recebimento correto das mensagens
- Define estrutura de mensageria orientada a eventos e sintaxe de baixo nível

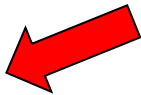


- Conteúdo das mensagens são codificadas utilizando chave-valor
 - Chave e valor separados pelo símbolo “|”
 - Chaves ficam do lado esquerdo do separador e os valores do lado direito
 - Nome das chaves faz parte da especificação do padrão
 - Especificações definem também os tipos de dados aceitos
 - Dados podem ser multivalorados
 - Valores apresentados em uma ordem específica
 - Pode conter campos vazios

Resultado de exame de glicose e dados demográficos de um paciente

```
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>
```

Identificador do
segmento da
mensagem (chave)



```
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>
```

Conteúdo do
segmento da
mensagem (valores)



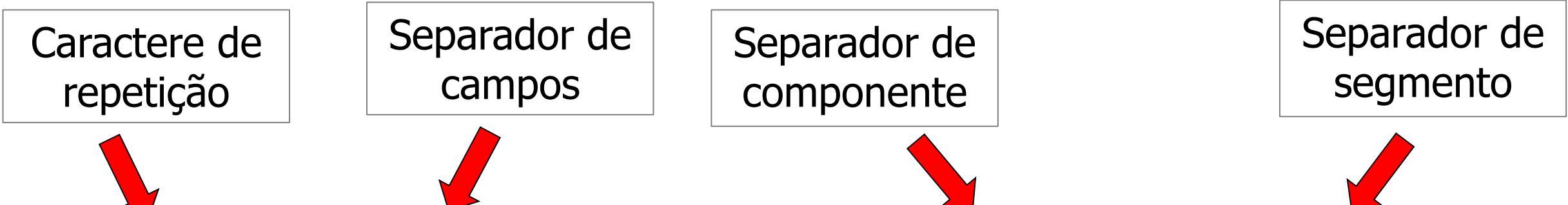
```
MSH|^~\&|GHH LAB|ELAB-3|GHH OE|BLDG4|200202150930||ORU^R01|CNTRL-3456|P|2.4<cr>  
PID|||555-44-4444|EVERYWOMAN^EVE^E^^^L|JONES|19620320|F|||153 FERNWOOD DR.^  
^STATESVILLE^OH^35292|(206)3345232|(206)752-121|||AC555444444||67-  
A4335^OH^20030520<cr>  
OBR|1|845439^GHH OE|1045813^GHH LAB|15545^GLUCOSE|||200202150730|||  
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>
```

Caractere de
repetição

Separador de
campos

Separador de
componente

Separador de
segmento

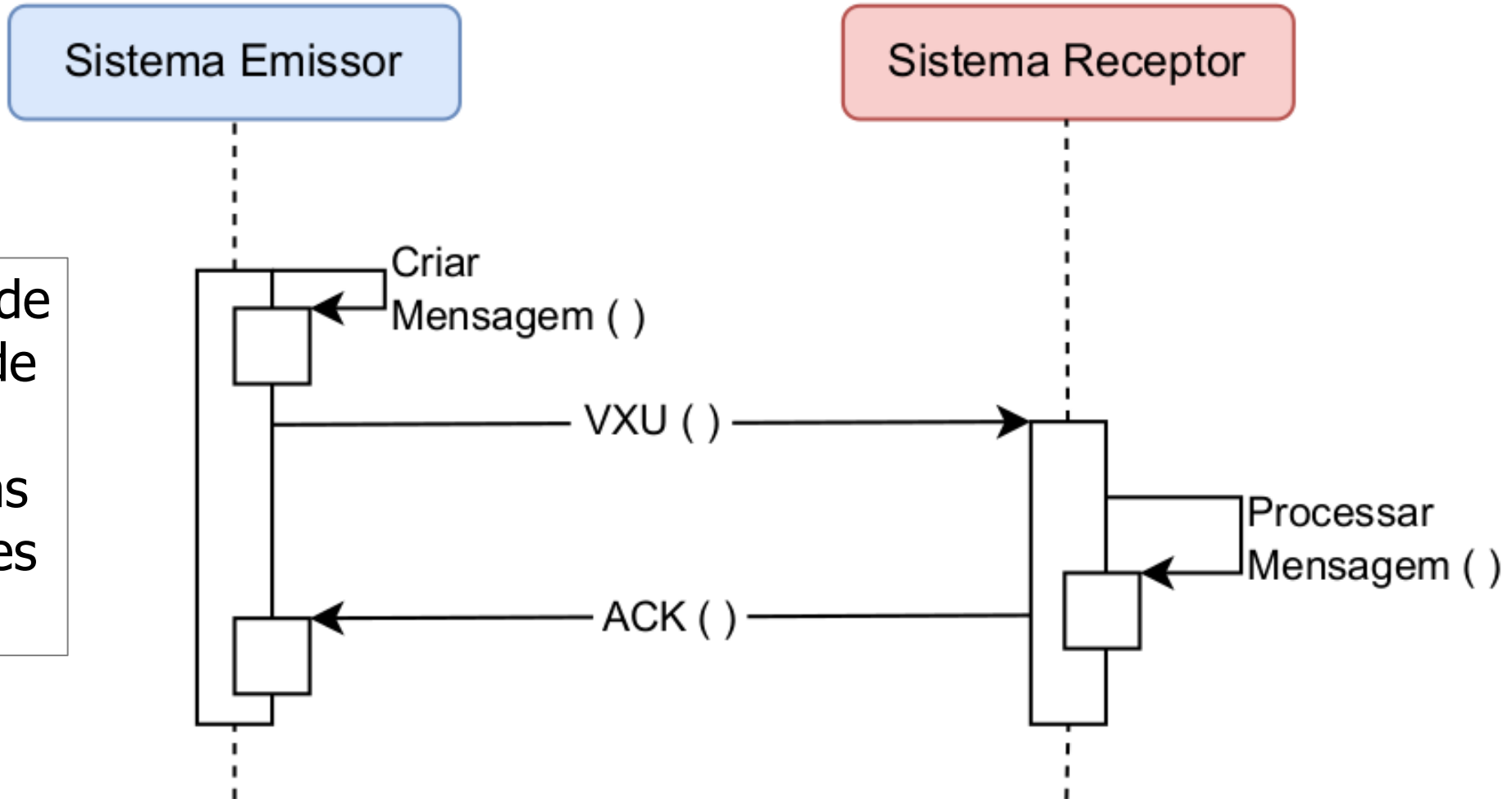


```
MSH|^~\&|GHH LAB|ELAB-3|GHH OE|BLDG4|200202150930||ORU^R01|CNTRL-3456|P|2.4<cr>
PID|||555-44-4444|EVERYWOMAN^EVE^E^^^L|JONES|19620320|F|||153 FERNWOOD DR.^
^STATESVILLE^OH^35292|(206)3345232|(206)752-121|||AC555444444||67-
A4335^OH^20030520<cr>
OBR|1|845439^GHH OE|1045813^GHH LAB|15545^GLUCOSE|||200202150730|||
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>
```

Fluxo do HL7 V2

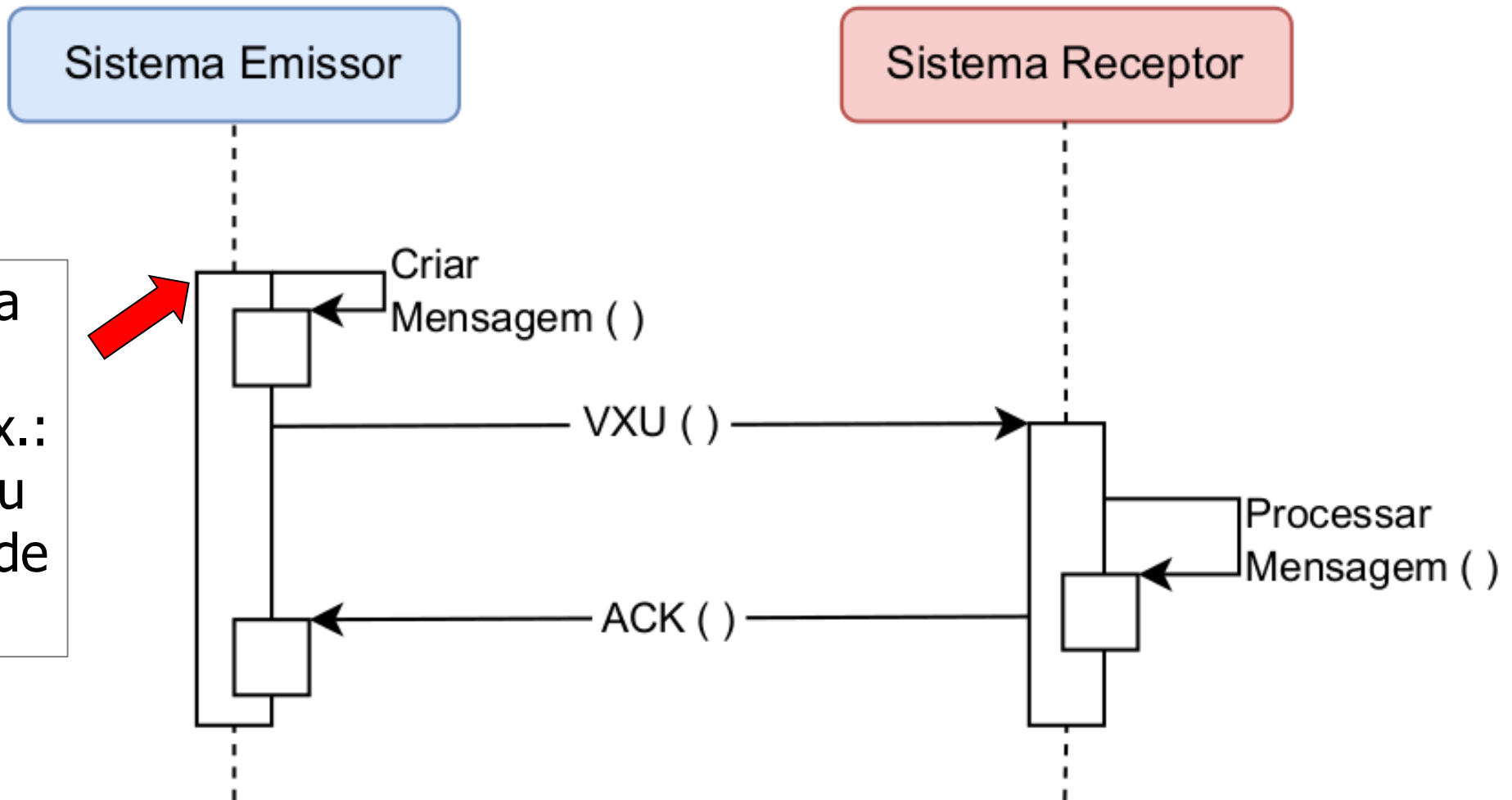
Exemplo

Transferência de informações de imunização entre sistemas de informações de saúde



Fluxo do HL7 V2

Exemplo



Evento gera a criação de mensagem (Ex.: atualização ou novo registro de vacinação)

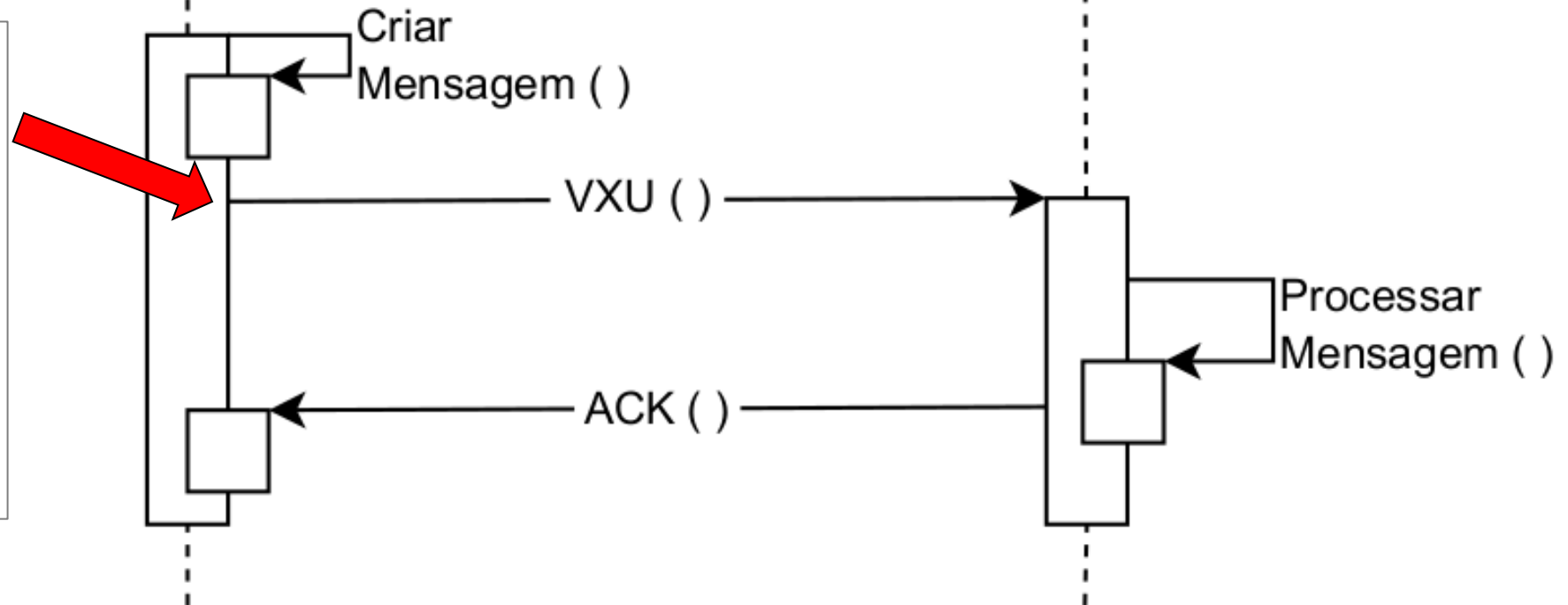
Fluxo do HL7 V2

Exemplo

Sistema Emissor

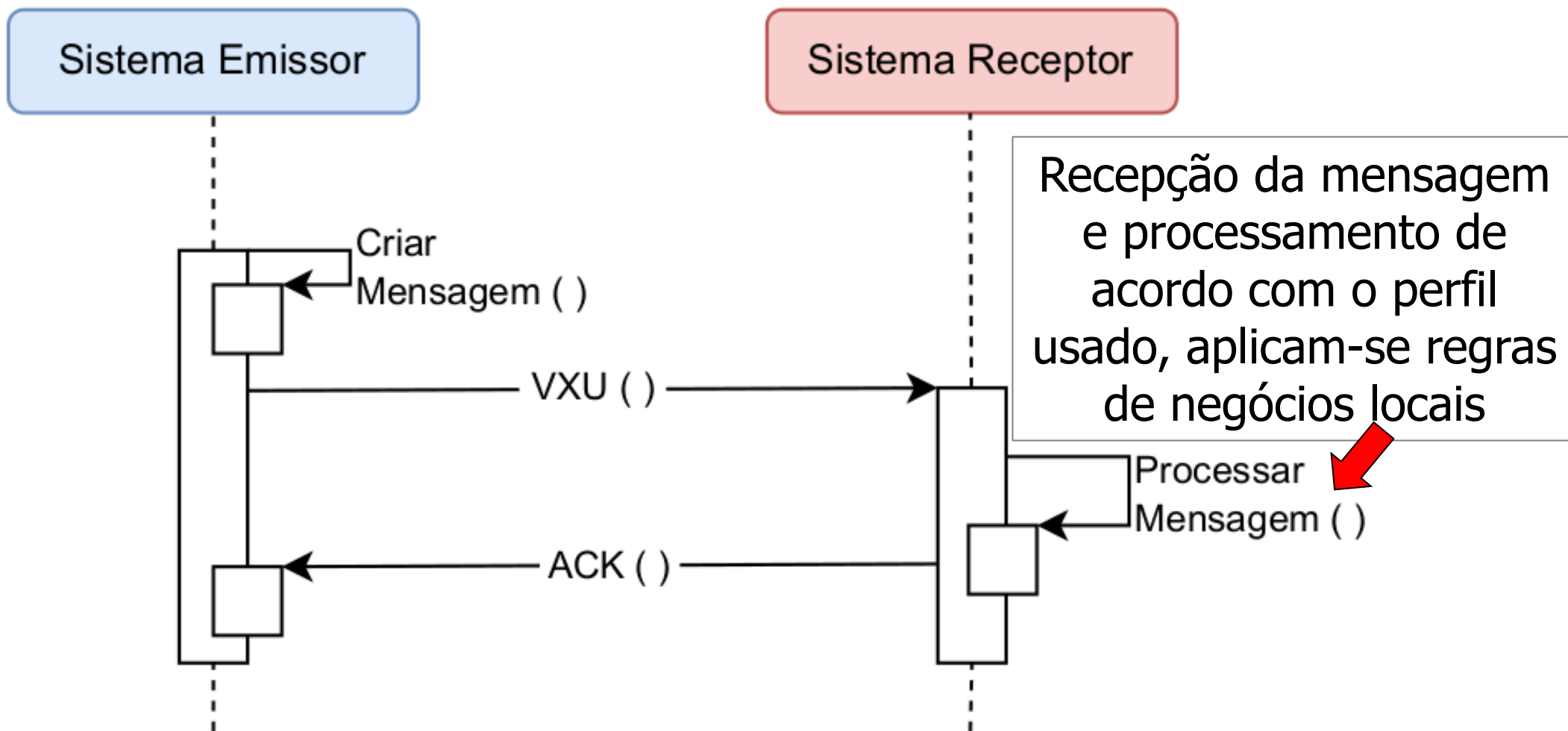
Sistema Receptor

Envio de mensagem de atualização de vacinação: registro de imunização atualizado



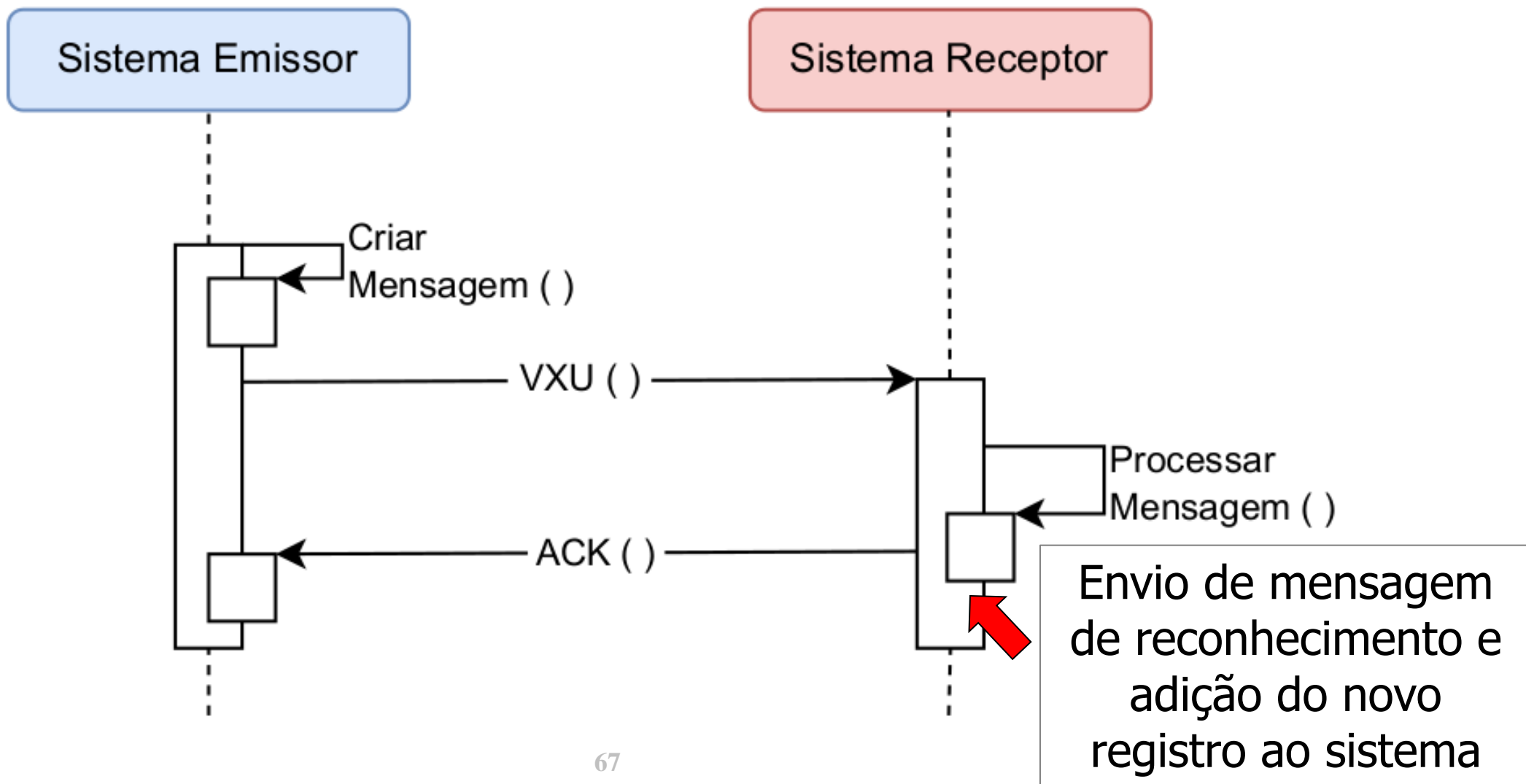
Fluxo do HL7 V2

Exemplo



Fluxo do HL7 V2

Exemplo



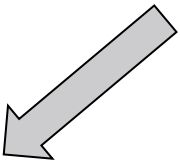
- Evolução do HL7 V2
 - Mensagens com conteúdo de mais alto nível
 - Voltado para sistemas com modelagem orientada a objetos
 - Conteúdo expresso em XML, mensagens maiores que no HL7 V2
 - Ganho de expressividade e semântica nas mensagens
 - Facilidade de leitura e compreensão
 - Maior suporte a estruturas hierárquicas
 - Fluxos herdados do HL7 V2

```
<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"/>
```

...

Resultado de exame de glicose e dados demográficos de um paciente

Classes com identificadores
únicos especificados pelo padrão

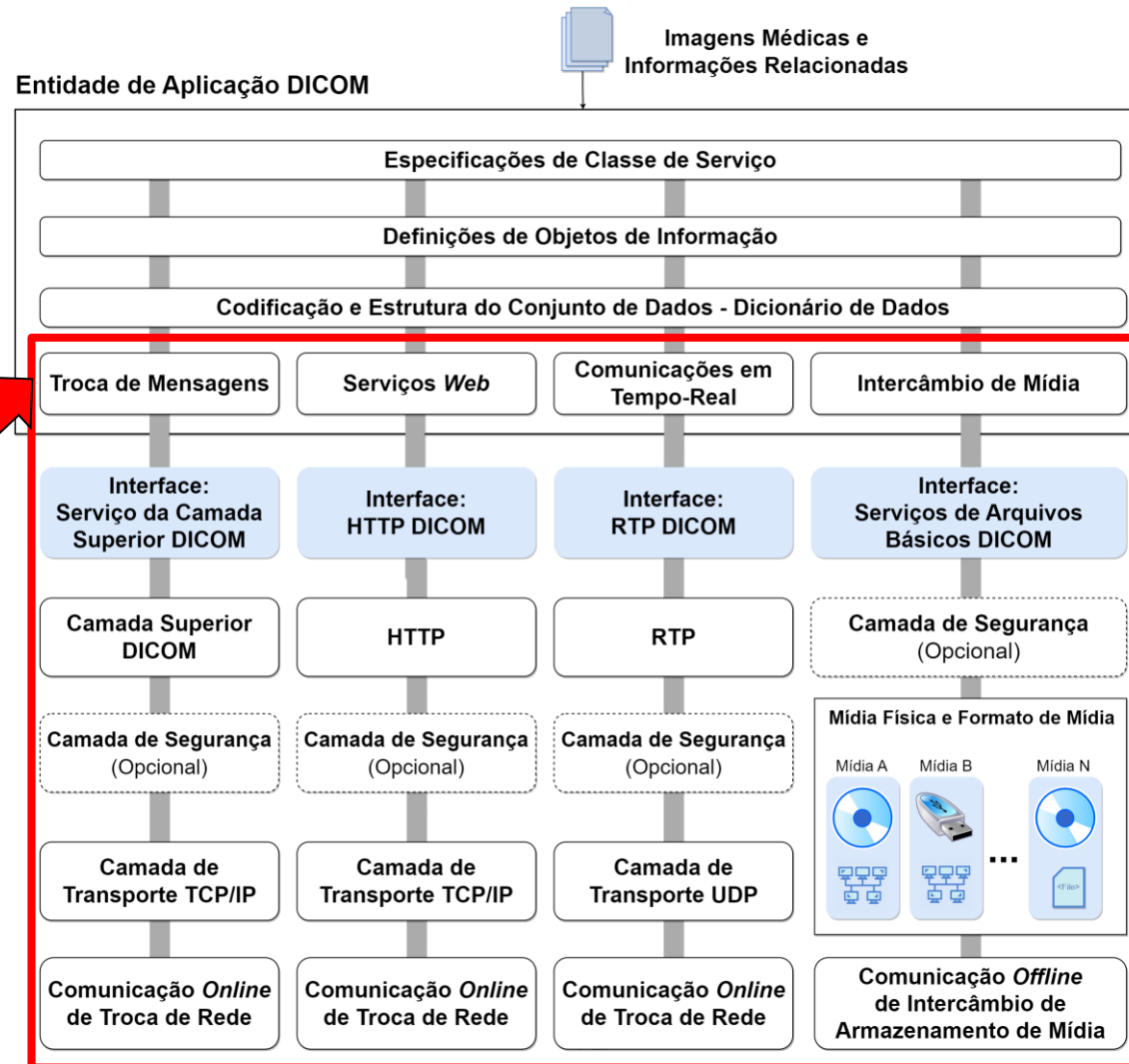


```
<observationEvent>  
  <id root="2.16.840.1.113883.19.1122.4" extension="1045813"  
    assigningAuthorityName="GHH LAB Filler Orders"/>  
  <code code="1554-5" codeSystemName="LN"  
    codeSystem="2.16.840.1.113883.6.1"  
    displayName="GLUCOSE^POST 12H CFST:MCNC:PT:SER/PLAS:QN"/>  
  <statusCode 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"/>
```

...

- Especifica um protocolo para troca de mensagens DICOM
 - Comunicação com as Classes de Serviço para as operações sobre os arquivos do padrão DICOM
 - Serviço de mensagens baseado no modelo OSI
- Executado sobre os protocolos TCP/IP
 - Permite comunicação via Internet

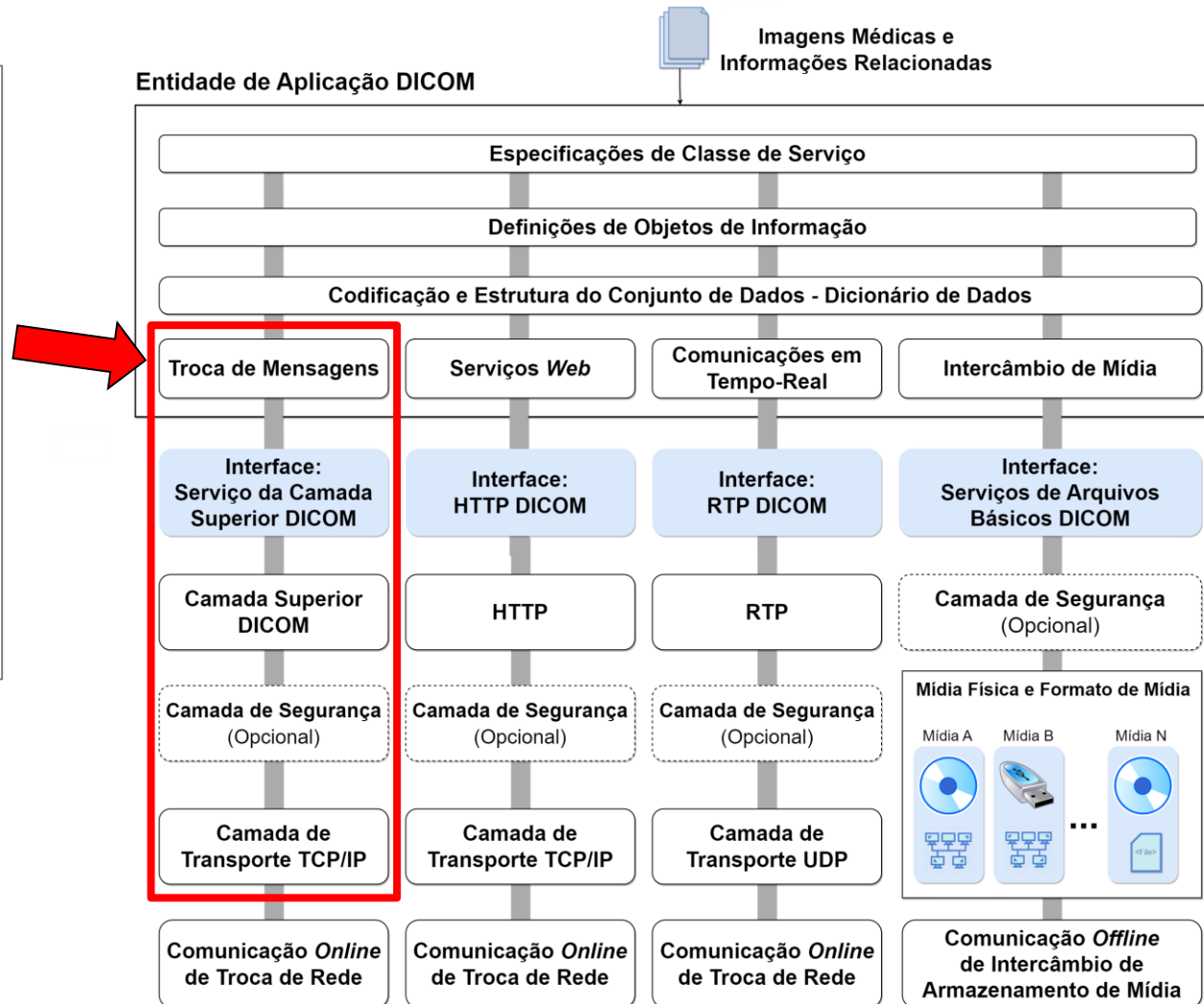
Modelo Geral dos Serviços DICOM



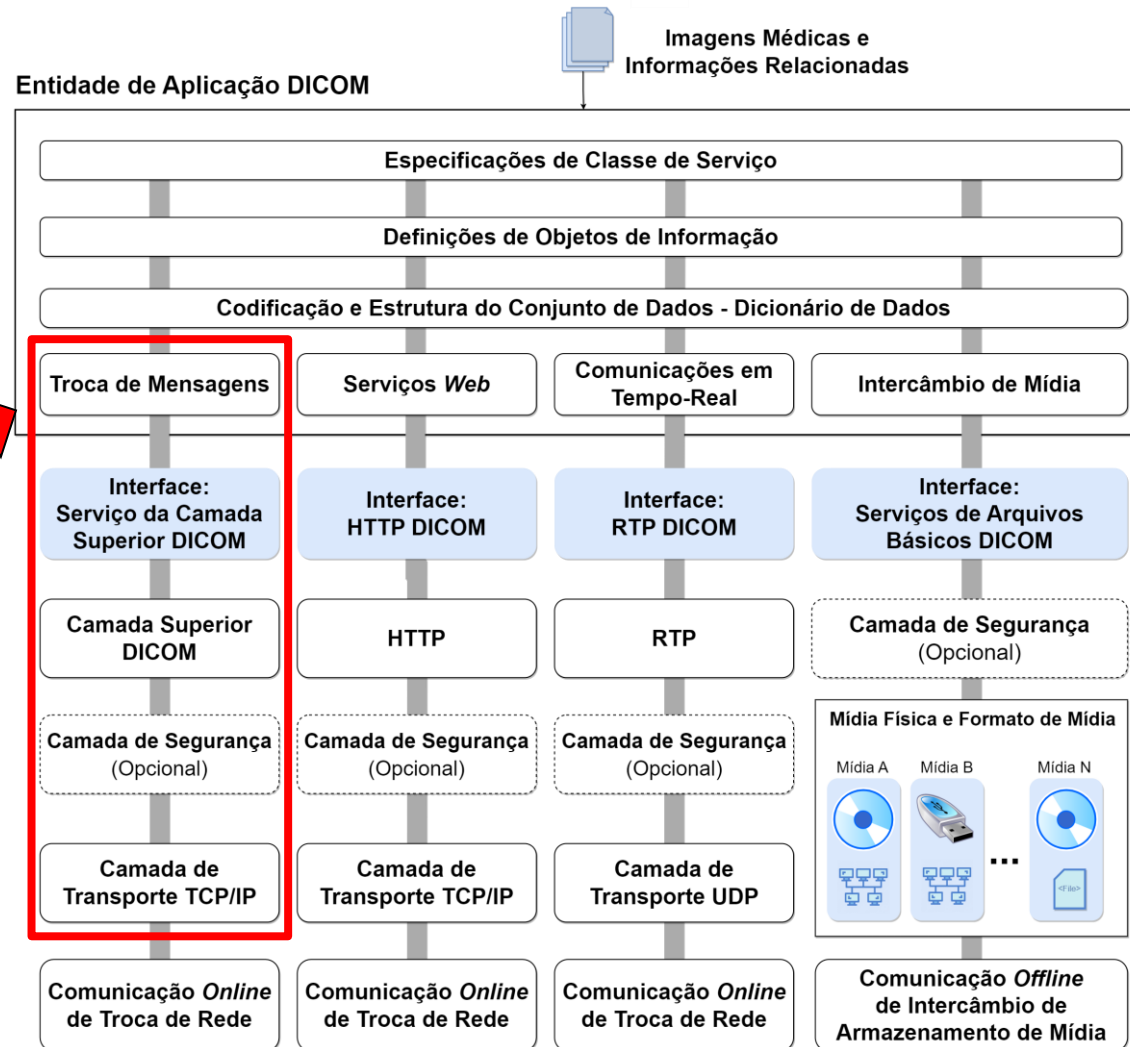
Conjunto de especificações do Serviço de Comunicação

Modelo Geral dos Serviços DICOM

Suporte para a troca de mensagens e notificações relativas aos serviços sobre as imagens médicas



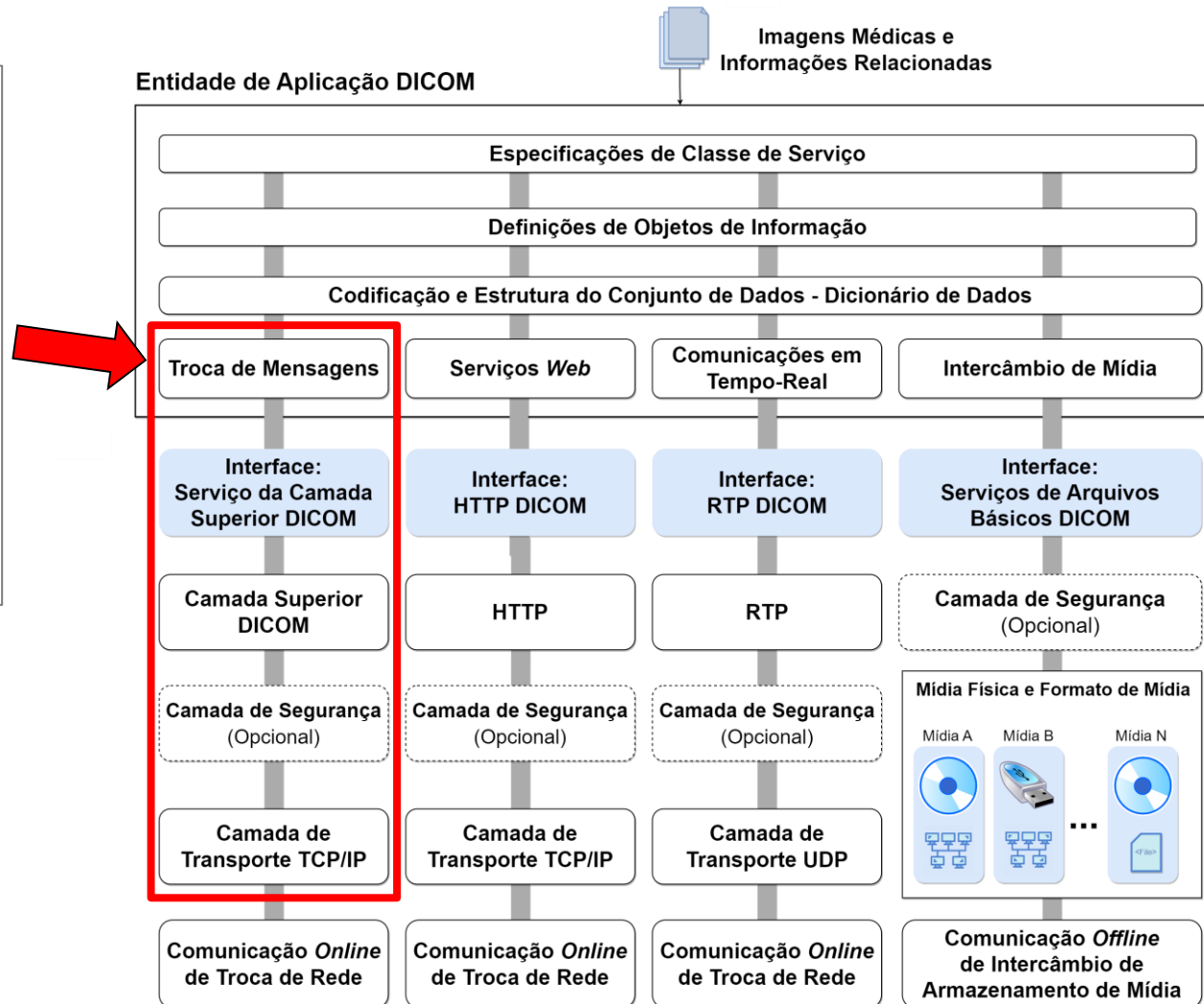
Modelo Geral dos Serviços DICOM



Serviço não genérico,
aceitando apenas
mensagens no
formato DICOM

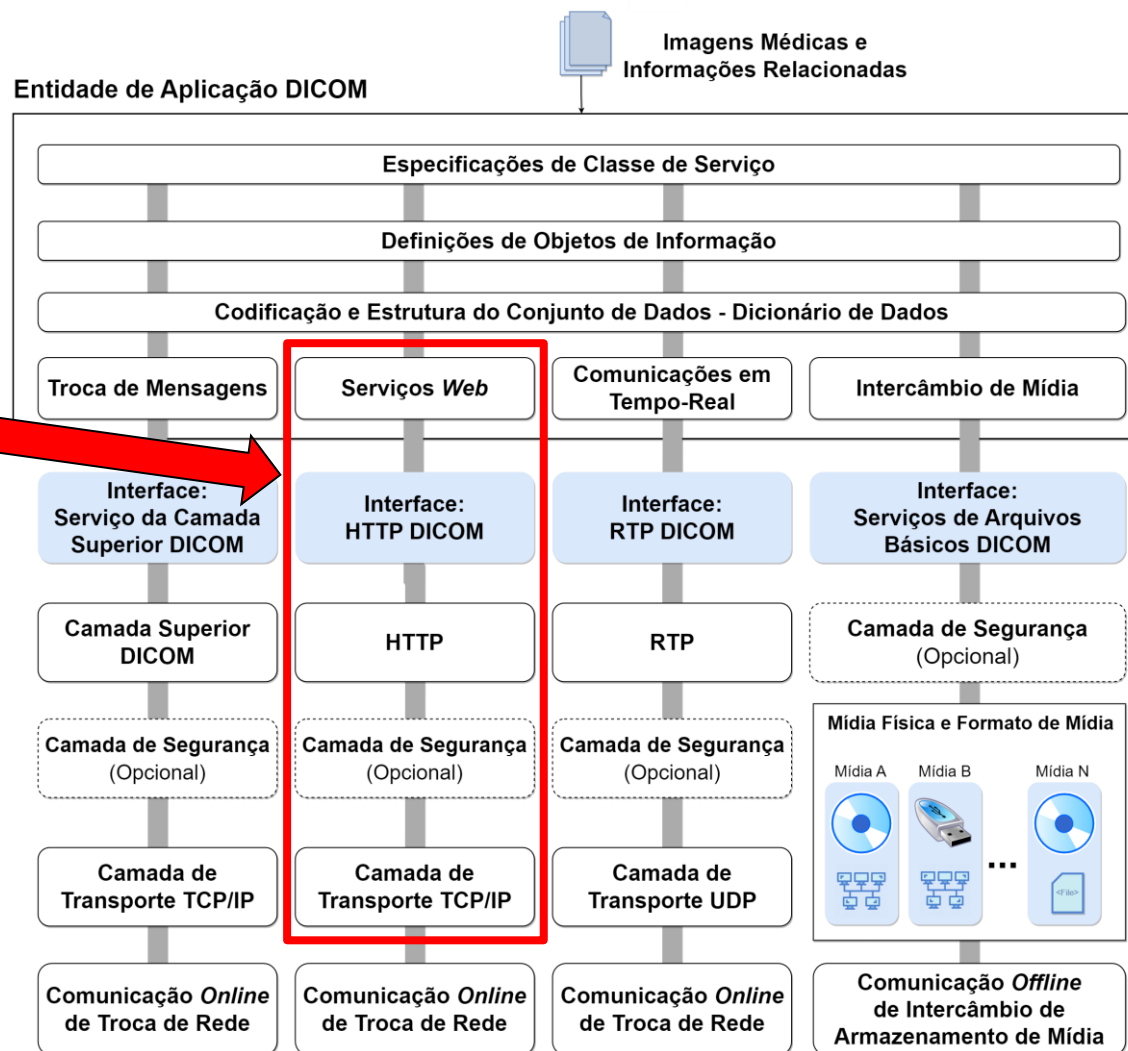
Modelo Geral dos Serviços DICOM

Implementa funcionalidades das camadas de aplicação, apresentação e sessão do modelo OSI

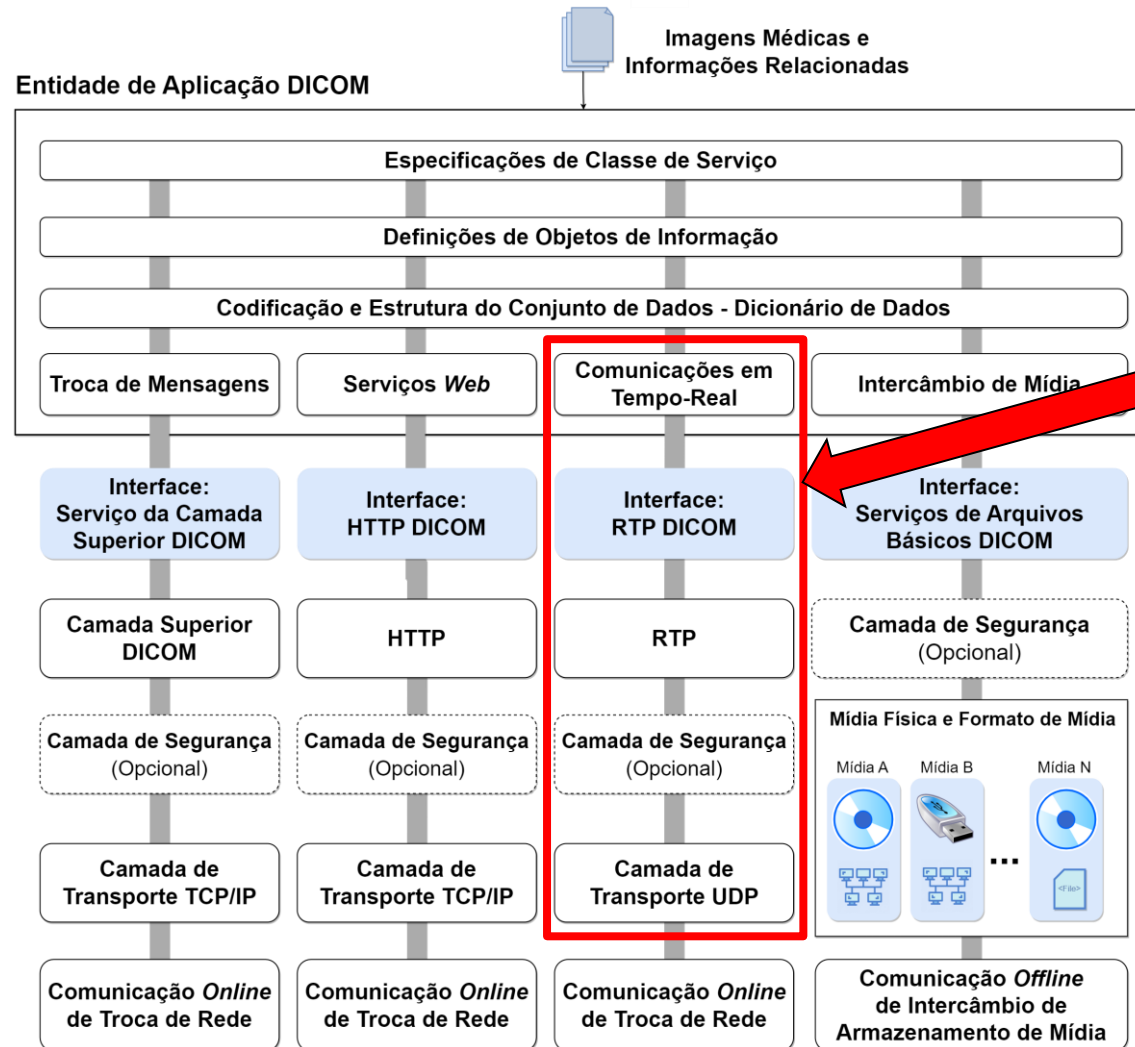


Modelo Geral dos Serviços DICOM

Suporte para serviços *web* (Ex.: disponibilização e consulta online dos arquivos)

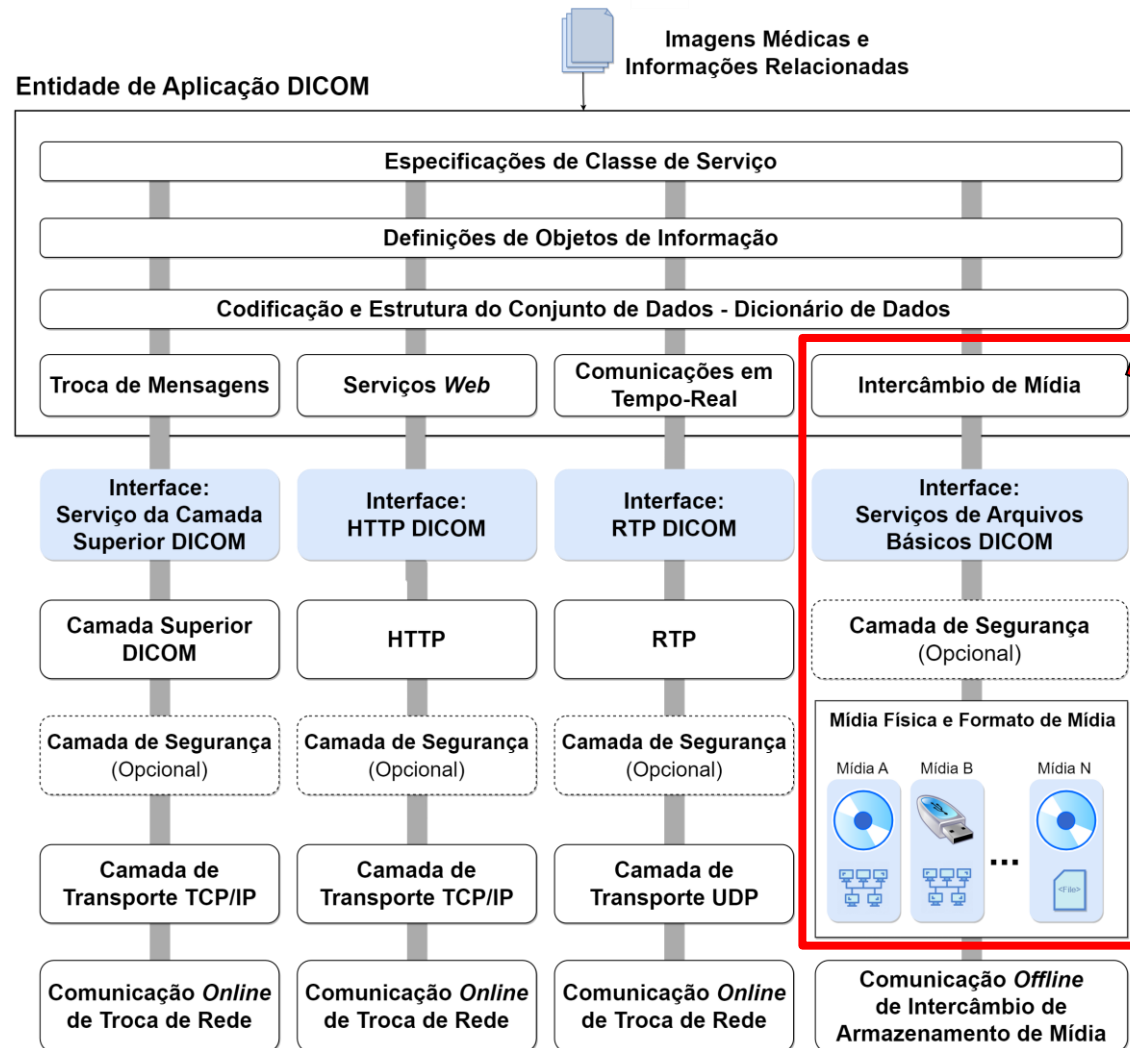


Modelo Geral dos Serviços DICOM



Suporte para transmissão em tempo real das mídias

Modelo Geral dos Serviços DICOM



Suporte para disponibilização de acesso offline às mídias

- **Objetivos**

- Definir um vocabulário comum
- Evitar ambiguidade e aumentar a clareza dos conteúdos armazenados nos registros médicos
- Definir um conjunto de **códigos e sistemas de classificação** que **representam conceitos de saúde**

• Características

- Padrão de codificação de procedimentos médicos
 - Foco na definição de código e nomenclatura dos procedimentos médicos
- Organizado em grupos e sub-grupos de procedimentos
- Utilizado em planos de saúde privados no Brasil
- Disponibilizado pela ANS em forma de tabela do Microsoft Excel



Tabela TUSS

Terminologia de Procedimento e Eventos em Saúde

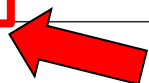
CÓDIGO	TUSS GRUPOS	TUSS SUBGRUPOS	PROCEDIMENTO
10101012	CONSULTAS	CONSULTAS	Em consultório (no horário normal ou preestabelecido)
10101012	CONSULTAS	CONSULTAS	Em consultório (no horário normal ou preestabelecido)
10101012	CONSULTAS	CONSULTAS	Em consultório (no horário normal ou preestabelecido)
10101020	CONSULTAS	CONSULTAS	Em domicílio
10101039	CONSULTAS	CONSULTAS	Em pronto socorro
10102019	CONSULTAS	VISITAS	Visita hospitalar (paciente internado)
10103015	CONSULTAS	RECÉM-NASCIDO	Atendimento ao recém-nascido em berçário
10103031	CONSULTAS	RECÉM-NASCIDO	Atendimento ao recém-nascido em sala de parto (parto normal ou operatório de alto risco)
10103023	CONSULTAS	RECÉM-NASCIDO	Atendimento ao recém-nascido em sala de parto (parto normal ou operatório de baixo risco)
10104011	CONSULTAS	UTI	Atendimento do intensivista diarista (por dia e por paciente)



Tabela TUSS

Terminologia de Procedimento e Eventos em Saúde

CÓDIGO	TUSS GRUPOS	TUSS SUBGRUPOS	PROCEDIMENTO
10101012	CONSULTAS	CONSULTAS	Em consultório (no horário normal ou preestabelecido)
10101012	CONSULTAS	CONSULTAS	Em consultório (no horário normal ou preestabelecido)
10101012	CONSULTAS	CONSULTAS	Em consultório (no horário normal ou preestabelecido)
10101020	CONSULTAS	CONSULTAS	Em domicílio
10101039	CONSULTAS	CONSULTAS	Em pronto socorro
10102019	CONSULTAS	VISITAS	Visita hospitalar (paciente internado)
10103015	CONSULTAS	RECÉM-NASCIDO	Atendimento ao recém-nascido em berçário
10103031	CONSULTAS	RECÉM-NASCIDO	Atendimento ao recém-nascido em sala de parto (parto normal ou operatório de alto risco)
10103023	CONSULTAS	RECÉM-NASCIDO	Atendimento ao recém-nascido em sala de parto (parto normal ou operatório de baixo risco)
10104011	CONSULTAS	UTI	Atendimento do intensivista diarista (por dia e por paciente)



Código do procedimento

Tabela TUSS

Terminologia de Procedimento e Eventos em Saúde

CÓDIGO	TUSS GRUPOS	TUSS SUBGRUPOS	PROCEDIMENTO
10101012	CONSULTAS	CONSULTAS	Em consultório (no horário normal ou preestabelecido)
10101012	CONSULTAS	CONSULTAS	Em consultório (no horário normal ou preestabelecido)
10101012	CONSULTAS	CONSULTAS	Em consultório (no horário normal ou preestabelecido)
10101020	CONSULTAS	CONSULTAS	Em domicílio
10101039	CONSULTAS	CONSULTAS	Em pronto socorro
10102019	CONSULTAS	VISITAS	Visita hospitalar (paciente internado)
10103015	CONSULTAS	RECÉM-NASCIDO	Atendimento ao recém-nascido em berçário
10103031	CONSULTAS	RECÉM-NASCIDO	Atendimento ao recém-nascido em sala de parto (parto normal ou operatório de alto risco)
10103023	CONSULTAS	RECÉM-NASCIDO	Atendimento ao recém-nascido em sala de parto (parto normal ou operatório de baixo risco)
10104011	CONSULTAS	UTI	Atendimento do intensivista diarista (por dia e por paciente)



Grupos e subgrupos

Tabela TUSS

Terminologia de Procedimento e Eventos em Saúde

CÓDIGO	TUSS GRUPOS	TUSS SUBGRUPOS	PROCEDIMENTO
10101012	CONSULTAS	CONSULTAS	Em consultório (no horário normal ou preestabelecido)
10101012	CONSULTAS	CONSULTAS	Em consultório (no horário normal ou preestabelecido)
10101012	CONSULTAS	CONSULTAS	Em consultório (no horário normal ou preestabelecido)
10101020	CONSULTAS	CONSULTAS	Em domicílio
10101039	CONSULTAS	CONSULTAS	Em pronto socorro
10102019	CONSULTAS	VISITAS	Visita hospitalar (paciente internado)
10103015	CONSULTAS	RECÉM-NASCIDO	Atendimento ao recém-nascido em berçário
10103031	CONSULTAS	RECÉM-NASCIDO	Atendimento ao recém-nascido em sala de parto (parto normal ou operatório de alto risco)
10103023	CONSULTAS	RECÉM-NASCIDO	Atendimento ao recém-nascido em sala de parto (parto normal ou operatório de baixo risco)
10104011	CONSULTAS	UTI	Atendimento do intensivista diarista (por dia e por paciente)



Especificação de contexto ou tipo de procedimento

• Características

- Padrão de **codificação de conceitos médicos**
 - Mais de 350 mil conceitos especificados
- Base de dados com consulta *online* mediante licenciamento pago
 - Salvo regiões ou órgãos já filiados a fundação
- Foco na **integração de terminologias** de vários países
- Especifica formas de implementar o armazenamento de dados das terminologias
- Serve de base para o desenvolvimento de aplicações

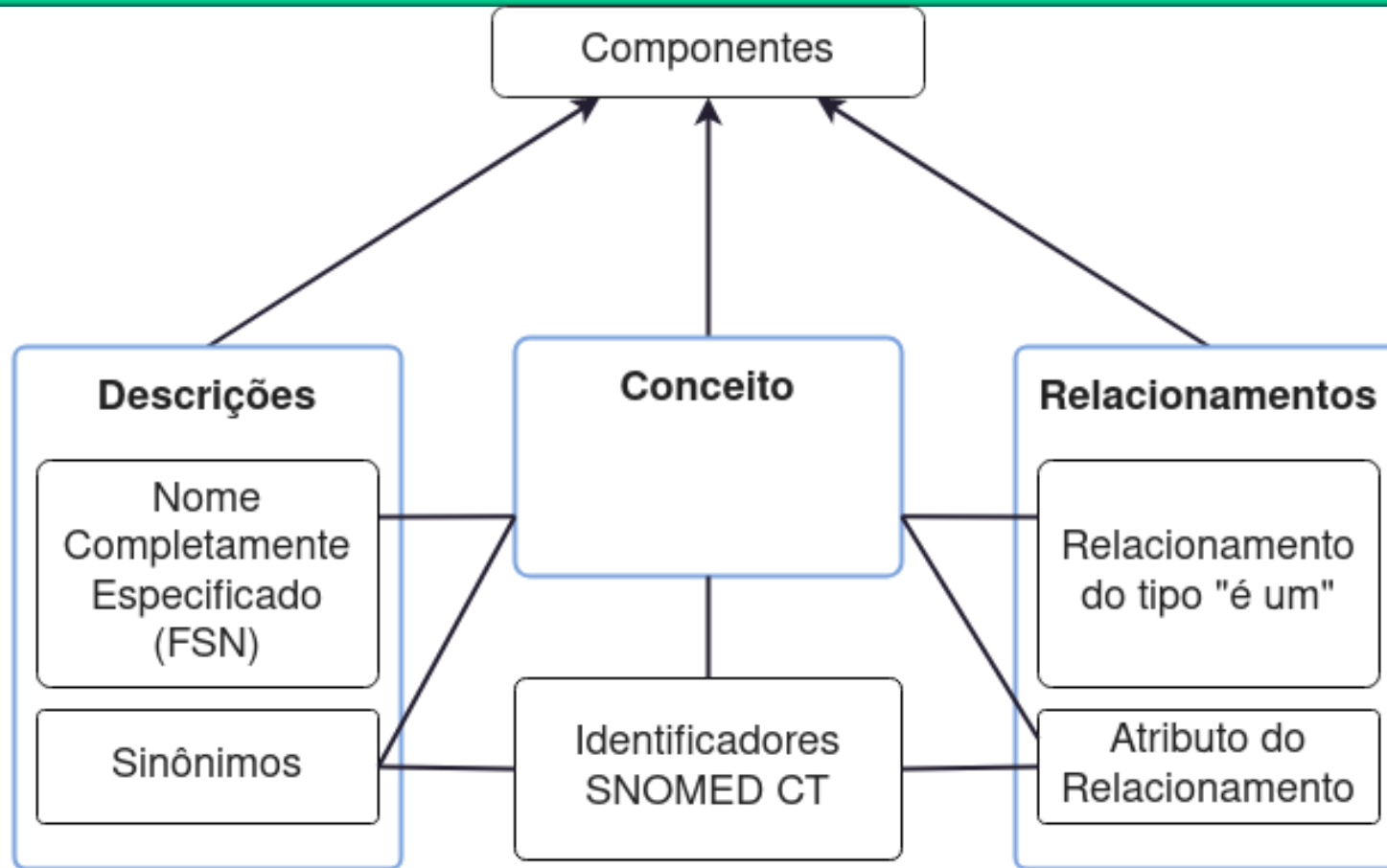


Systemized Nomenclature of Medicine Clinical Terms - SNOMED CT

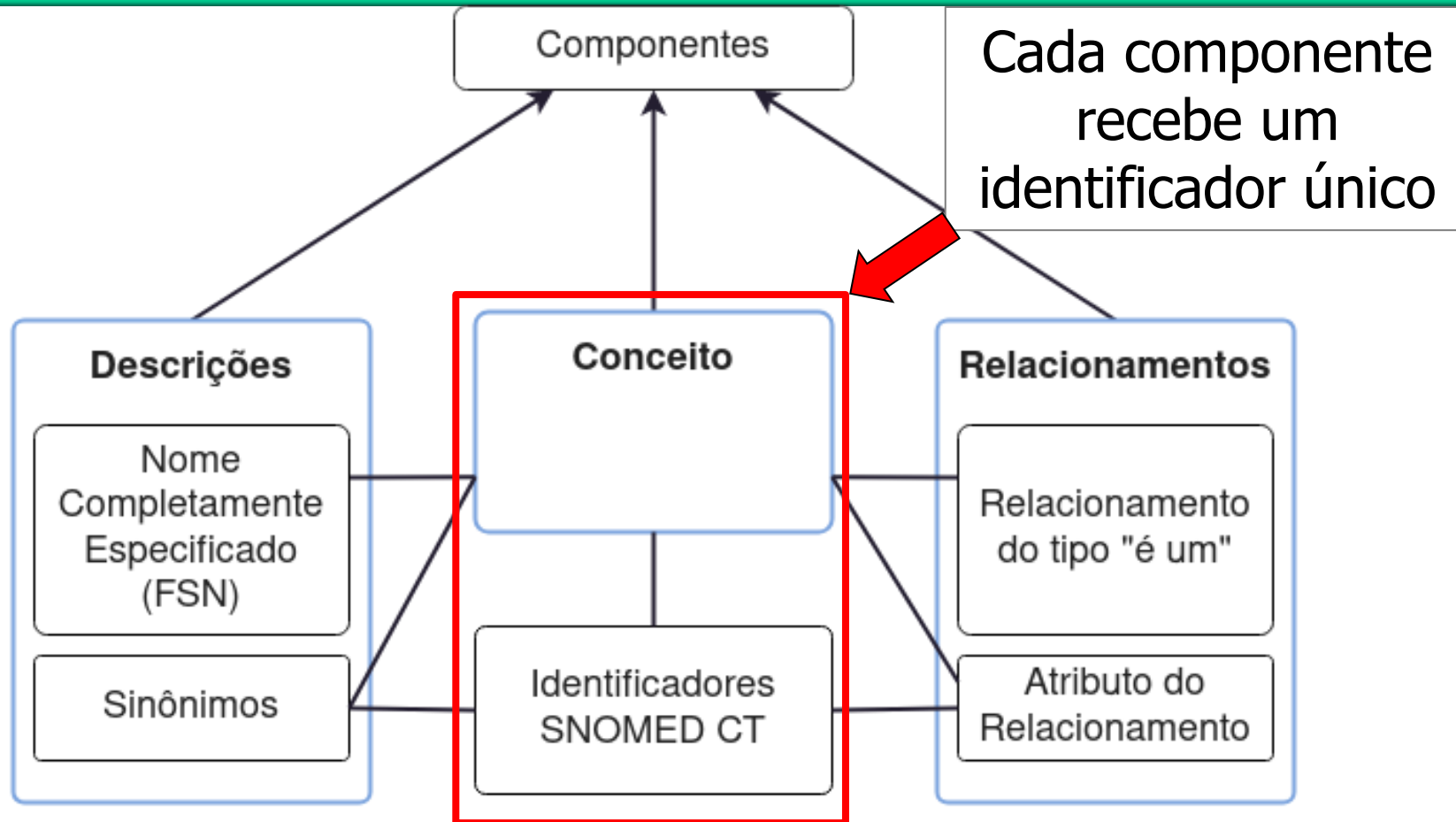
- Termos organizados em três componentes básicos
 - **Conceitos:** identificador único e computável
 - **Relacionamentos:** registra as relações entre os conceitos
 - Pode ser utilizado para representar hierarquias
 - **Descrições:** ideia clínica capturada de forma única e completa
 - Nome Completamente Especificado (Fully-Specified Name - FSN)



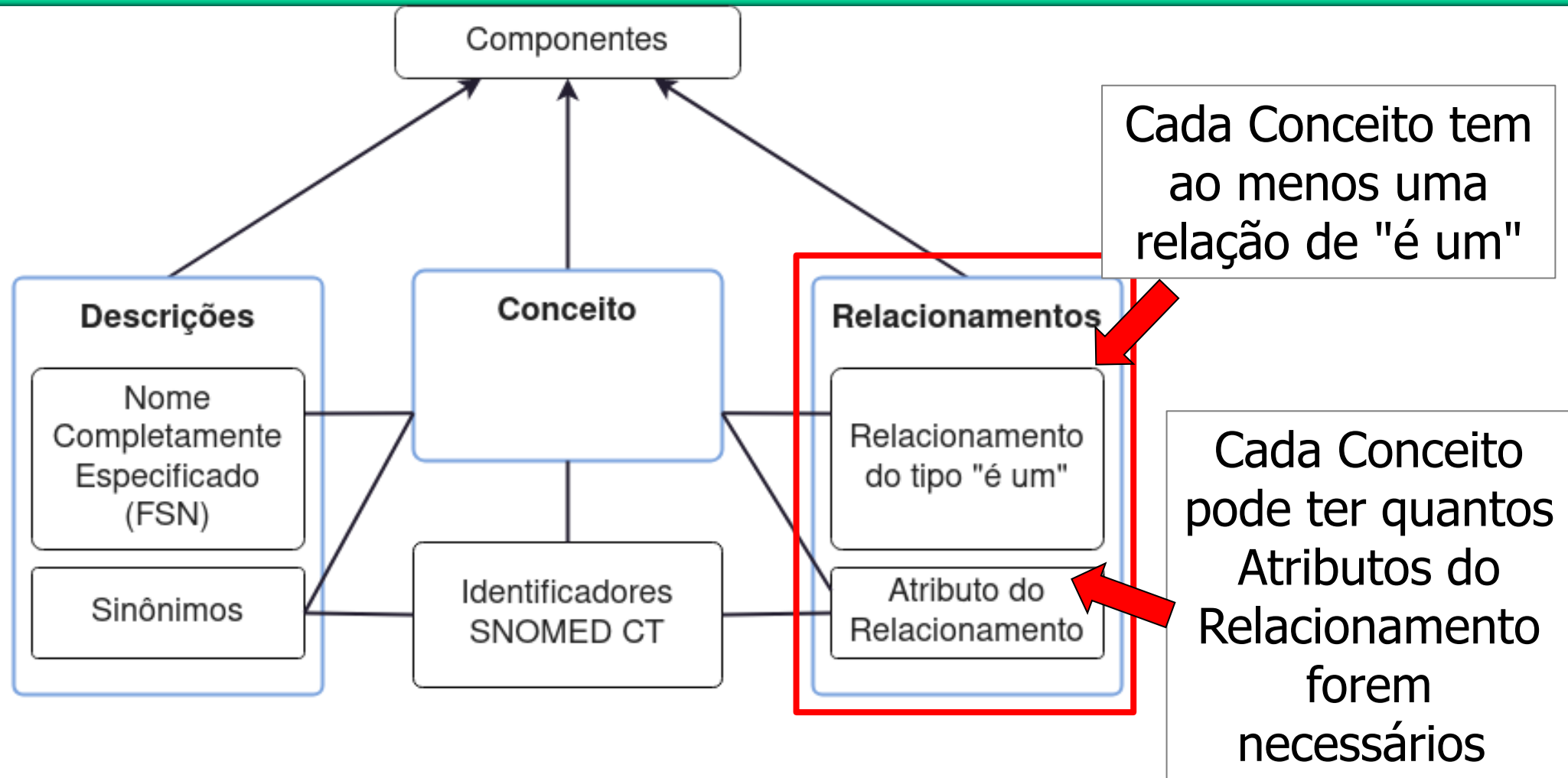
Systemized Nomenclature of Medicine Clinical Terms - SNOMED CT



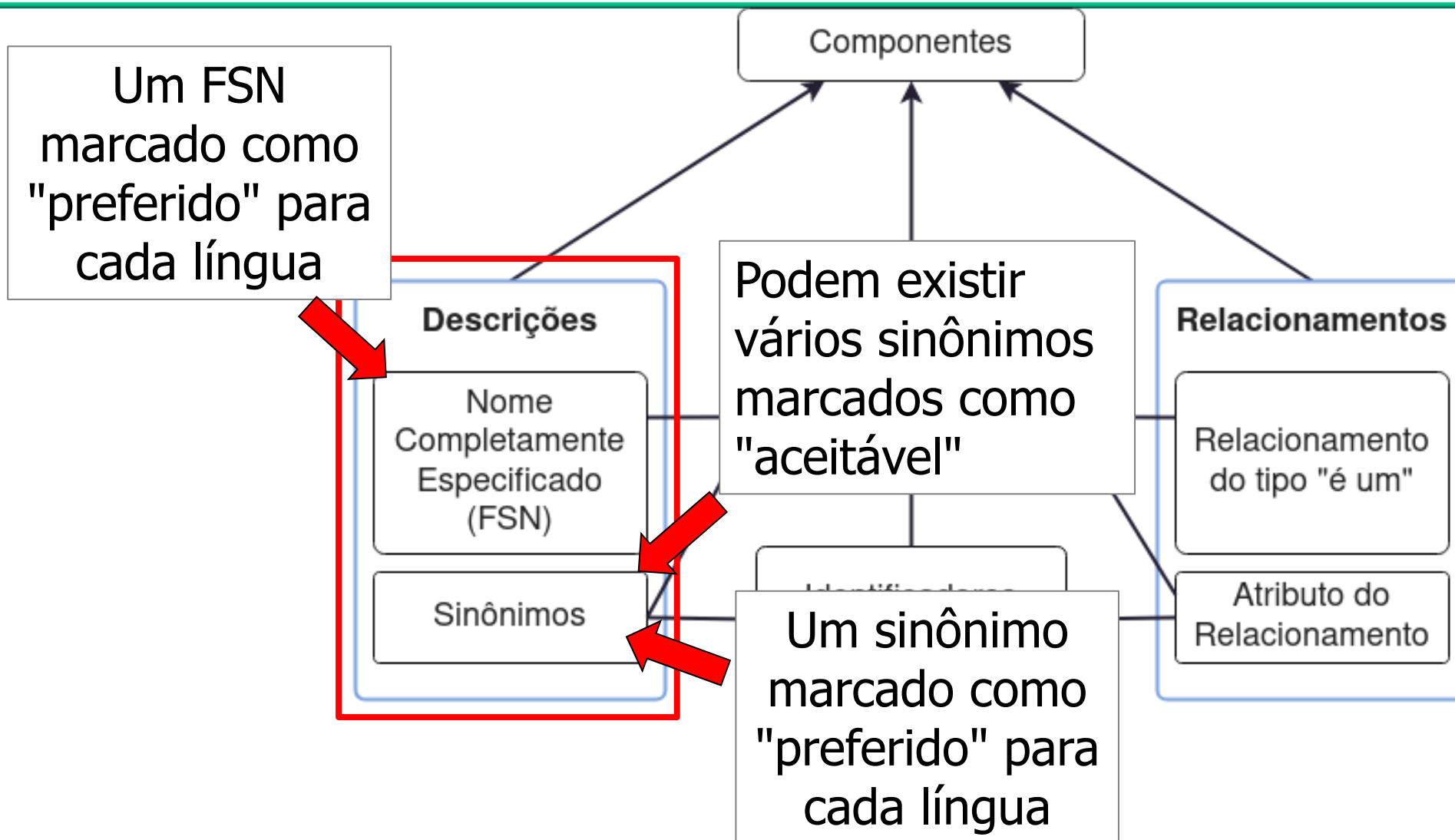
Systemized Nomenclature of Medicine Clinical Terms - SNOMED CT



Systemized Nomenclature of Medicine Clinical Terms - SNOMED CT



Systemized Nomenclature of Medicine Clinical Terms - SNOMED CT



• Características

- Padrão de **codificação de tipos de observação** para resultados de exames e testes laboratoriais
 - Foco na extinção da ambiguidade dos **campos de observação**
- Disponibiliza códigos e nomenclaturas
 - Através de uma API FHIR
 - Através de busca pelo site
 - Através de *download* da base completa
- Pode integrar com outras bases
 - SNOMED-CT

LOINC[®]
from Regenstrief

Logical Observation Identifiers Names and Codes - LOINC


- Nomenclatura baseada em uma lógica de seis dimensões
 - **Componente (ou Analito)**: substância ou entidade medida/observada
 - **Propriedade**: característica ou atributo do analito
 - **Tempo**: intervalo de tempo sobre o qual uma observação foi feita
 - **Sistema**: espécime ou substância sobre a qual a observação foi feita
 - **Escala**: como o valor da observação é quantificado ou expresso
 - **Método (opcional)**: classificação de alto nível de como a observação foi feita


Exemplo Termo do Código LOINC 806-0


Leukocytes:NCnc:Pt:CSF:Qn:Manual count


Fully-Specified Name (FSN)	Long Common Name (LCN)	Short Name
Leukocytes: NCnc: Pt: CSF: Qn: Manual count	Leukocytes [# /volume] in Cerebral spinal fluid by Manual count	WBC # CSF Manual



COMPONENTE (ANALITO)
Leukocytes (células brancas)


PROPRIEDADE
NCnc (Number concentration)


TEMPO
Pt (Point in time)


SISTEMA (ESPÉCIME)
CSF (Cerebral spinal fluid)


ESCALA
Qn (Quantitative)


MÉTODO
Manual Count

Mensagem HL7 V2 com Observação LOINC

Tipo de dado do resultado
(código HL7V2 OBX-5/CE)
informando que o campo é
um Elemento Codificado

Indicação de que é
um código LOINC

Indicação de que é
um código
SNOMED-CT

```
OBX|CE|57131-5^Newborn condition with pos markers^LN|7573000^PKU^SCT
```

Código HL7V2 para
valores de observação

Código LOINC
identificando a
observação

Código SNOMED-CT
identificando o resultado
(Fenilcetonúria)

• Características

- Suporte ao levantamento estatístico das causas de morte e morbidade no mundo
 - Desenvolvido pela OMS
 - Organizado de forma estatística e em hierarquia de doenças relacionadas
- Foco na definição dos códigos e nomes das doenças e problemas de saúde
- Disponibiliza os códigos e nomenclaturas
 - Através de uma API REST sobre HTTP
 - Através de busca pelo site oficial
 - Através de uma ferramenta de codificação

CID-10 no Brasil
ICD → internacional
CID → nacional



**World Health
Organization**

ICD-11 Ferramenta de Codificação

Navegação
hierárquica



- ▶ certain other consequences of external causes
- ▶ **23** External causes of morbidity or mortality
- ▶ **24** Factors influencing health status or contact with health services
- ▼ **25** Codes for special purposes
 - ▼ International provisional assignment of new diseases of uncertain aetiology and emergency use
 - ▶ **RA00** Conditions of uncertain aetiology and emergency use
 - ▼ **RA01** COVID-19
 - RA01.0** COVID-19, virus identified

Code: RA01.0 & XN161 / QA00.C / QC05.0

✓ Select

Coding Note

Use this code when infection with the COVID-19 virus (SARS-CoV-2) has been confirmed by laboratory testing irrespective of severity of clinical signs or symptoms.

Postcoordination

Infectious agent XN161 SARS-CoV-2 Omicron ✕

Associated with QA00.C Laboratory examination ✕

QC05.0 Isolation ✕

Infectious agent (use additional code, if desired .)

search in axis: Infectious

▼ XN109 SARS-CoV-2

XN0HL SARS-CoV-2 Alpha

XN4Q7 SARS-CoV-2 Beta

XN5BQ SARS-CoV-2 Gamma

Coronavirus disease 2019

Inclusions

Coronavirus disease 2019

ICD-11 Ferramenta de Codificação

certain other consequences of external causes

- ▷ 23 External causes of morbidity or mortality
- ▷ 24 Factors influencing health status or contact with health services
- ▽ 25 Codes for special purposes
 - ▽ International provisional assignment of new diseases of uncertain aetiology and emergency use
 - ▷ RA00 Conditions of uncertain aetiology and emergency use
 - ▽ RA01 COVID-19
 - RA01.0** COVID-19, virus identified

Code: RA01.0&XN161 / QA00.C / QC05.0

✓ Select

Coding Note

Use this code when infection with the COVID-19 virus (SARS-CoV-2) has been confirmed by laboratory testing irrespective of severity of clinical signs or symptoms.

Postcoordination

Infectious agent	XN161 SARS-CoV-2 Omicron	×
Associated with	QA00.C Laboratory examination	×
	QC05.0 Isolation	×

Infectious agent (use additional code, if desired .)

search in axis: Infectious

- ▽ XN109 SARS-CoV-2
 - XN0HL SARS-CoV-2 Alpha
 - XN4Q7 SARS-CoV-2 Beta
 - XN5BQ SARS-CoV-2 Gamma

Características da ocorrência

ICD-11 Ferramenta de Codificação

certain other consequences of external causes

- ▷ 23 External causes of morbidity or mortality
- ▷ 24 Factors influencing health status or contact with health services
- ▽ 25 Codes for special purposes
 - ▽ International provisional assignment of new diseases of uncertain aetiology and emergency use
 - ▷ RA00 Conditions of uncertain aetiology and emergency use
 - ▽ RA01 COVID-19
 - RA01.0** COVID-19, virus identified

Code: RA01.0&XN161 / QA00.C / QC05.0

✓ Select

Coding Note

Use this code when infection with the COVID-19 virus (SARS-CoV-2) has been confirmed by laboratory testing irrespective of severity of clinical signs or symptoms.

Postcoordination

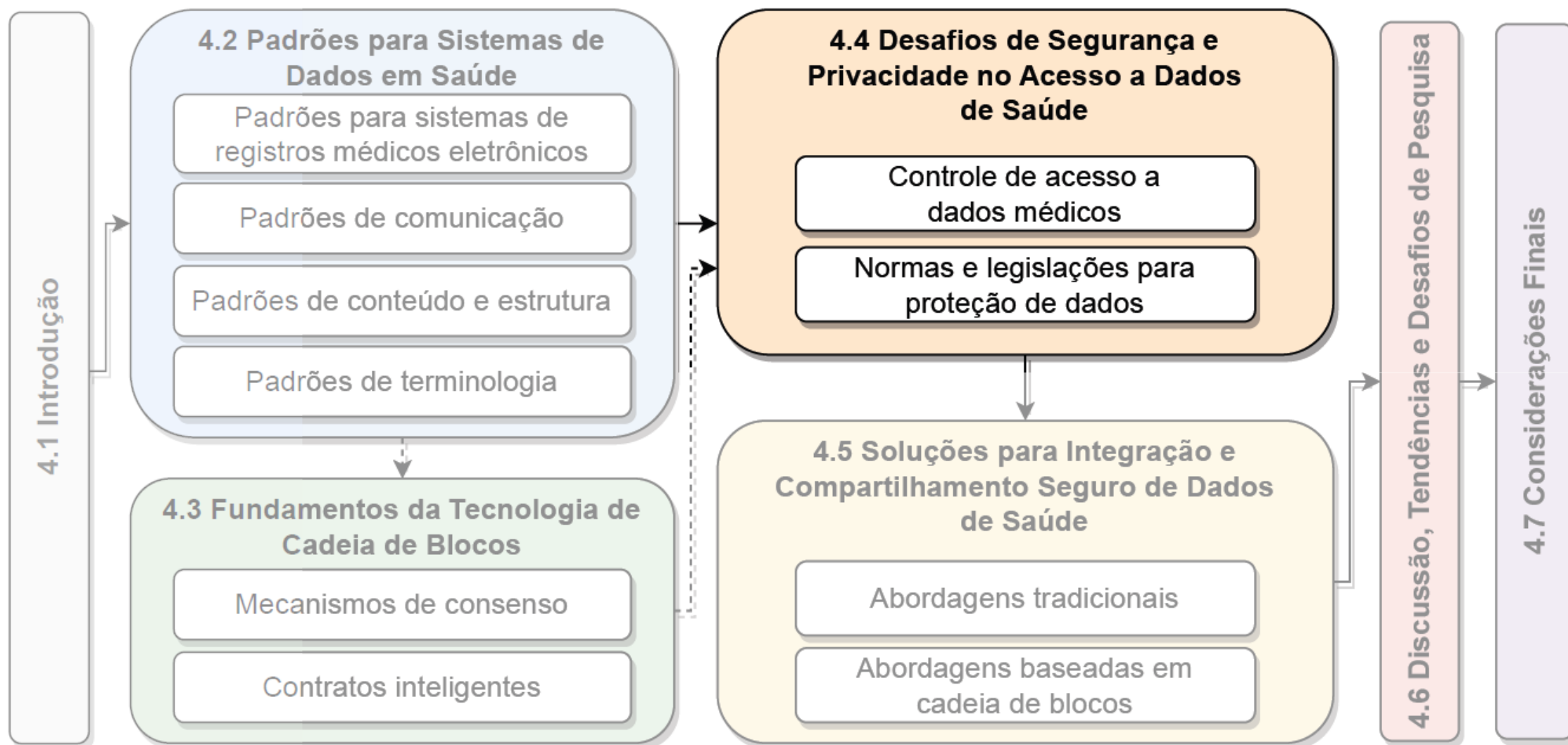
Infectious agent	XN161 SARS-CoV-2 Omicron	×
Associated with	QA00.C Laboratory examination	×
	QC05.0 Isolation	×

Infectious agent (use additional code, if desired .)

search in axis: Infectious

- ▽ XN109 SARS-CoV-2
 - XN0HL SARS-CoV-2 Alpha
 - XN4Q7 SARS-CoV-2 Beta
 - XN5BQ SARS-CoV-2 Gamma

Código Gerado é a junção da doença com as características



Desafios de Segurança e Privacidade no Acesso a Dados de Saúde

- **Registros Médicos (Dados pessoais)** → Monetização
 - **Compartilhado com outras entidades**
 - Problemas na guarda e segurança das informações
 - *Quem acessou, quando acessou, por que acessou?*
 - **Roubo de informações**
 - Espionagem industrial
 - Venda para Governos

Negligência e Ingenuidade

Acesso a Dados de Saúde

Desafios de Segurança e Privacidade

- Registros Médicos Eletrônicos → **A quem pertencem?**
 - **Ao paciente!**
- Hospitais, clínicas entre outros → **Controladores dos dados**
- **Gerenciamento de Identidade**
 - Aumento da confiança e privacidade
 - Maior complexidade → Tende a ser centralizado
 - **Ponto único de falha**
 - **Processos ineficientes**

- **Sistemas de registros médicos eletrônicos**

- **Sofrem das mesmas** dores de diversos sistemas informatizados
 - Compartilhamento de senhas
 - Senhas fracas
 - Pouca ou nenhuma auditoria
- **Compartilhamento de dados**
 - Inseguro
 - Entidades não confiáveis
 - Sem autorização do dono dos dados



Acesso a Dados de Saúde

Desafios de Segurança e Privacidade

- **Confidencialidade**
 - Dados devem ser acessados somente por pessoas específicas
- **Integridade**
 - Dados adulterados ou errôneos podem ser fatais
- **Disponibilidade**
 - Indispensável para tratamentos adequados

Controle de Acesso

- Existem diversos mecanismos de controle de acesso a registros médicos
 - Fornecer os níveis de permissão adequados
 - Agrupar usuários conforme perfis
 - Criar políticas de acesso

- Sistemas que executam tarefas de **Autenticação** e **Autorização**

- **Autenticação**

- Processo para definir se alguém ou algo é o que diz ser
 - Realizado através da comparação das credenciais fornecidas por outra previamente validada

- **Autorização**

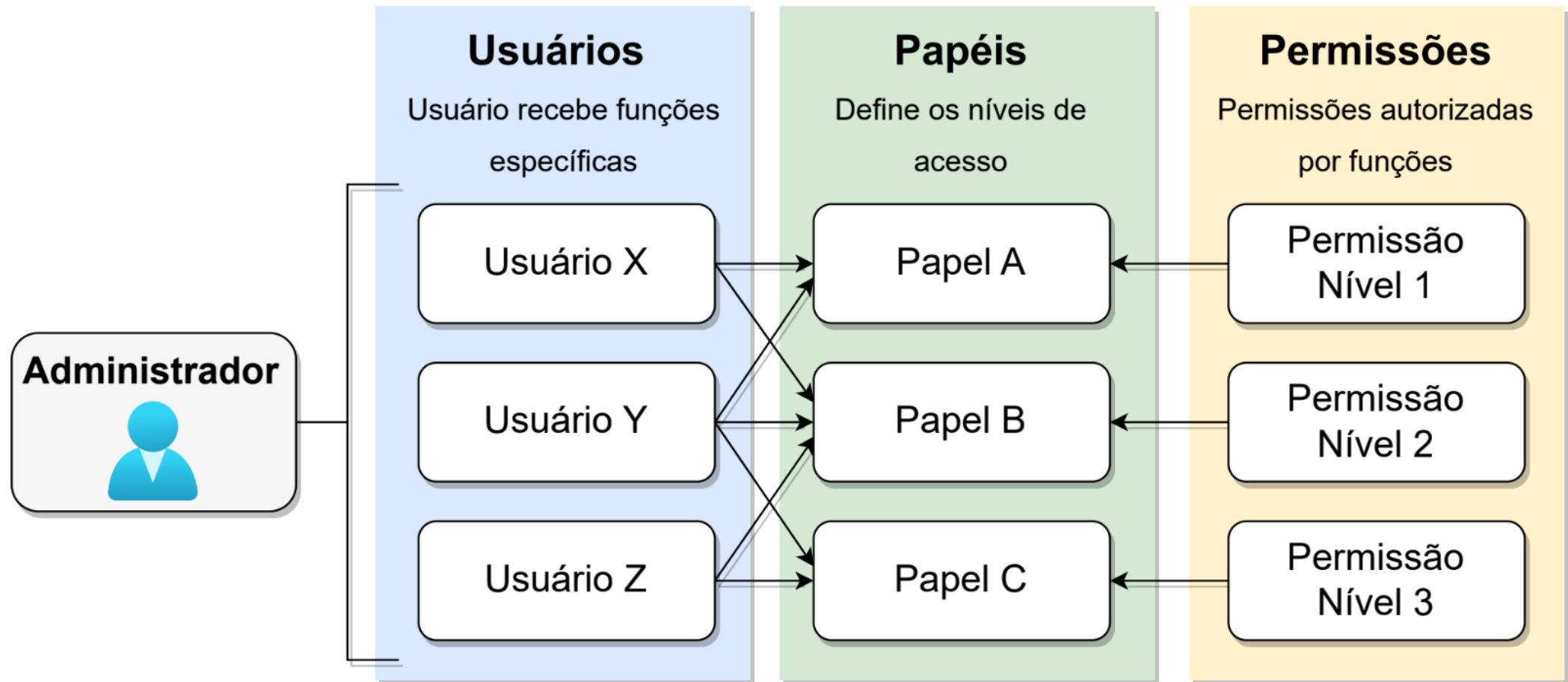
- Processo para impor políticas
 - Determinar quais tipos de atividades um usuário já autenticado pode executar



- **RBAC** → Controle de acesso baseado em papéis
 - Cada usuário pode possuir mais de uma função ou papel
 - Administrador central
 - Complexidade → **Gerenciar múltiplos grupos e usuários**
 - Gera um problema de escalabilidade
 - Impacta na segurança → Fornece o mesmo nível para todos!
- **Variações**
 - **E-RBAC** → visa aumentar a segurança em situações de emergência

Controle de Acesso a Dados Médicos

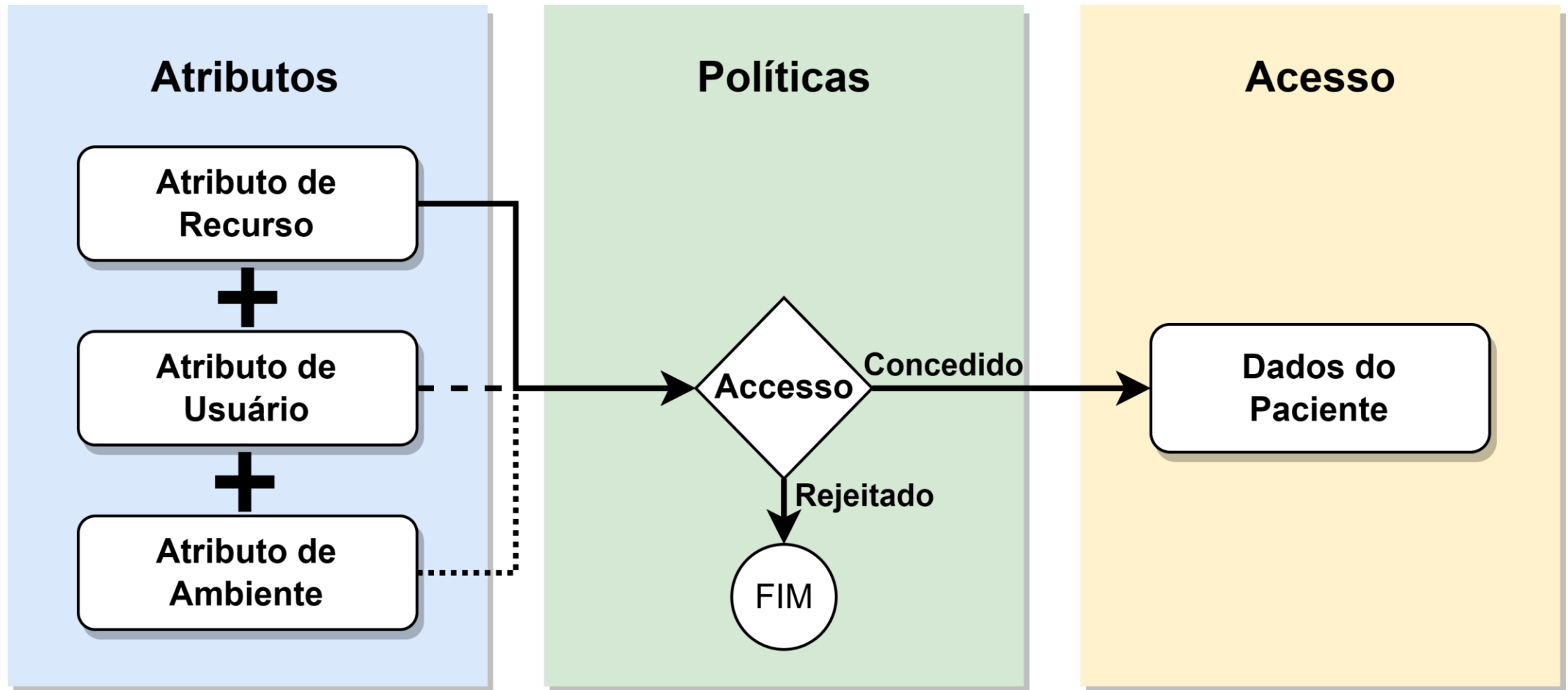
RBAC



- **ABAC** → Controle de acesso baseado em atributos
 - Políticas consistem em combinações lógicas de atributos
 - Usuários precisam estar em bases de dados: LDAP, AD etc
 - Cada usuário é associado a atributos previamente definidos
 - **Atributos**
 - Recurso --> Data de criação, nome do recurso a ser acessado
 - Usuário --> Informações como nome, cargo, função etc.
 - Ambiente --> Informações geográficas
 - **Políticas**
 - Concessão
 - Negação

Controle de Acesso a Dados Médicos

ABAC

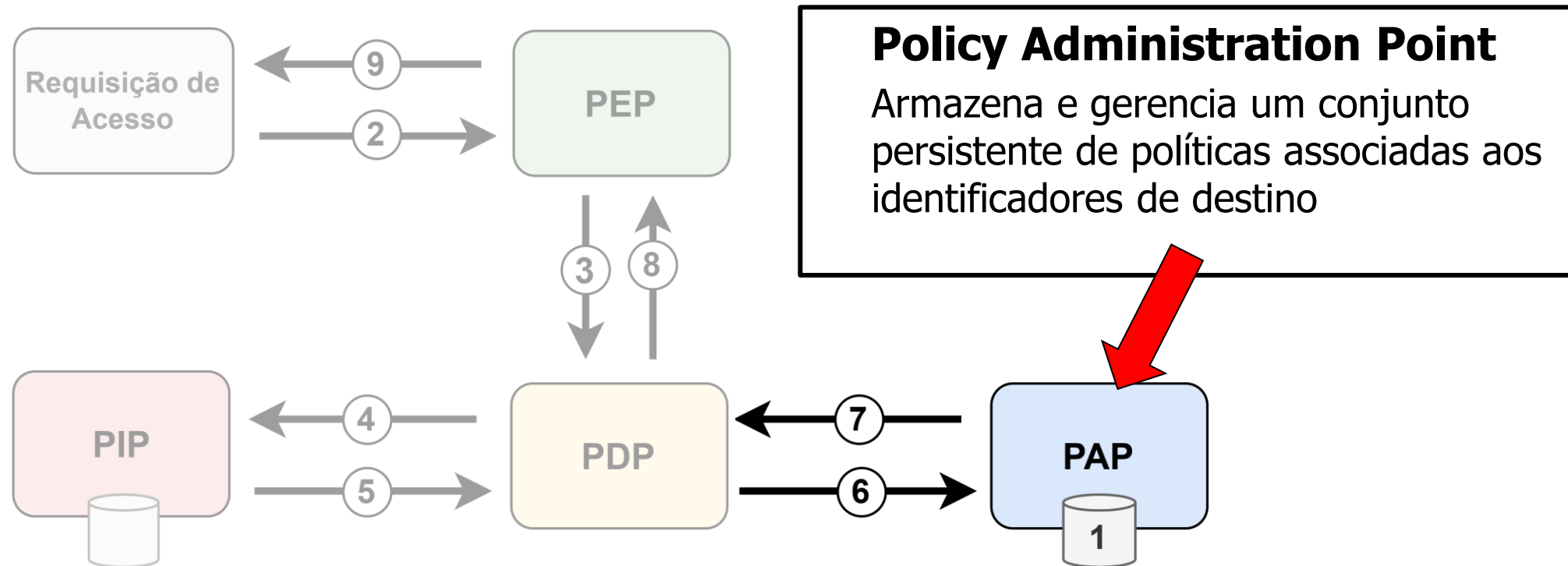


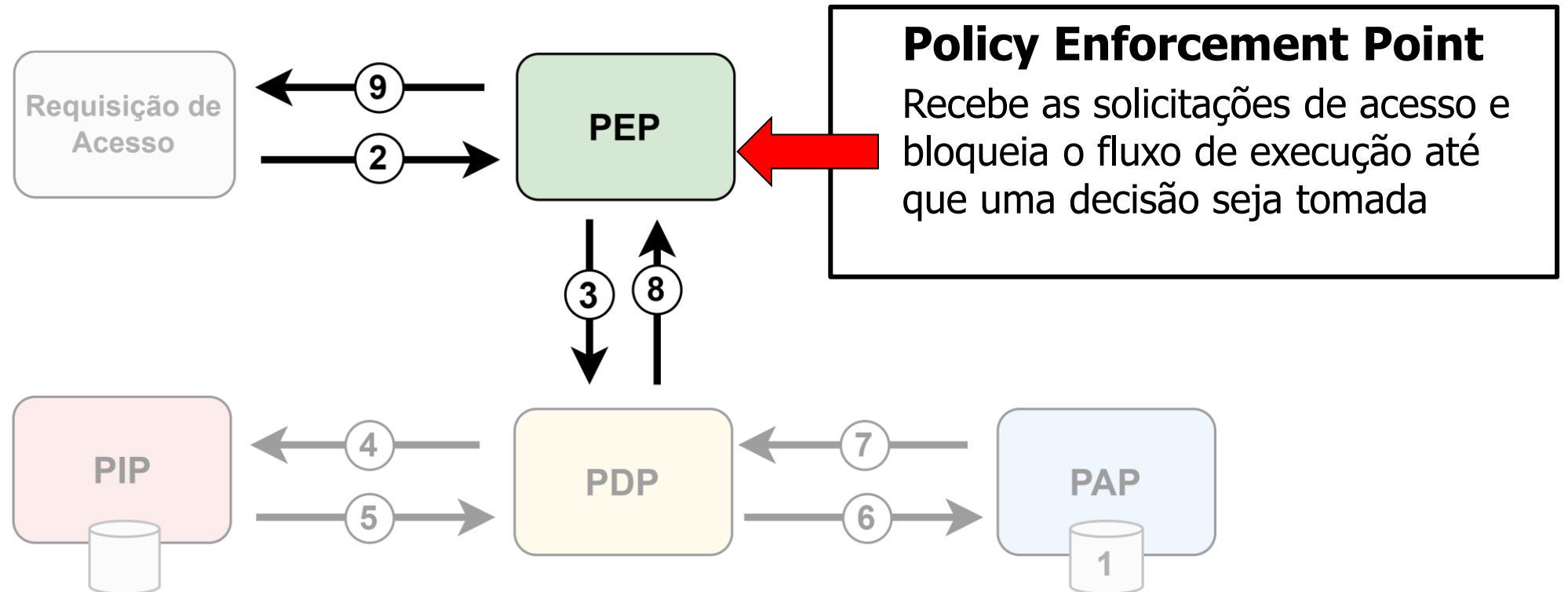
- **SitBAC** → Controle de acesso baseado em situação
 - Considera a situação atual do paciente
 - Permissão mediante solicitações
 - Avalia o solicitante dos dados, a tarefa a ser executada, a autorização legal, entre outros
 - Pode ser utilizado em conjunto com o RBAC, uma vez que se trata de uma generalização
 - Desafios em questões de segurança

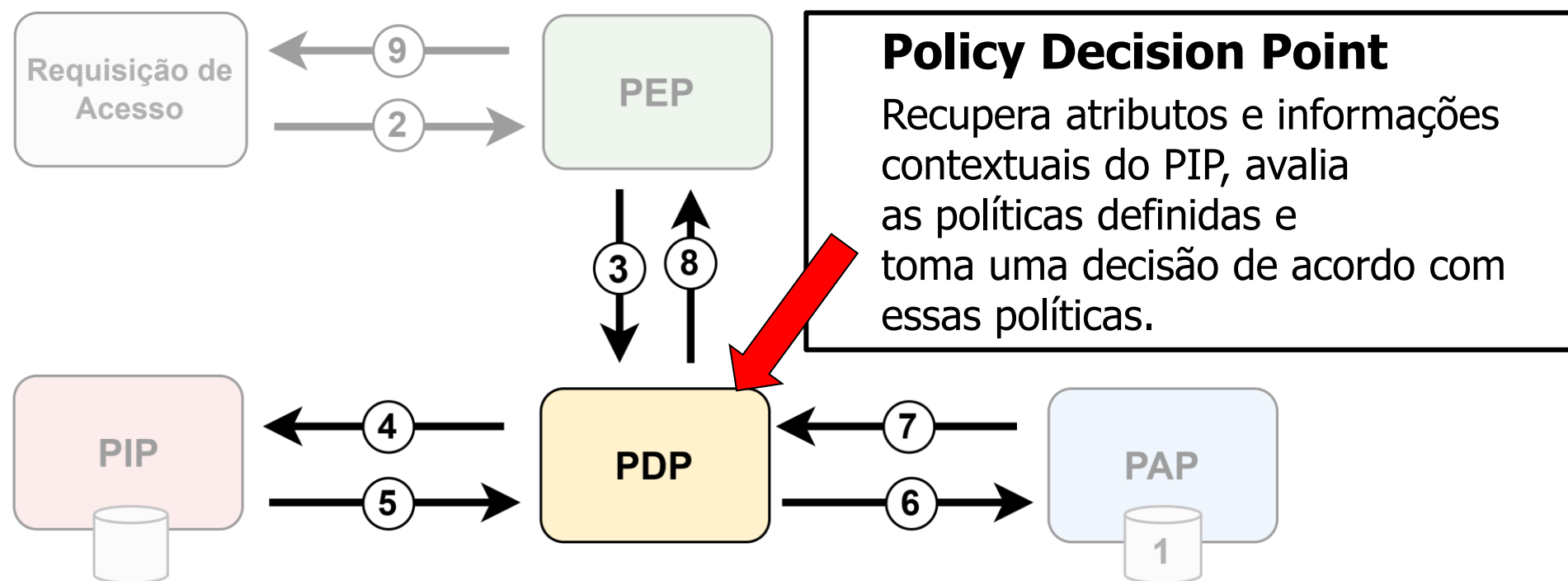
- **WBAC** → Controle de acesso baseado em trabalho
 - Foco no trabalho a ser executado
 - Permissões são modificadas a cada tratamento a ser realizado
 - Usuários são atribuídos a papéis ou equipes
 - Complexidade no gerenciamento de tarefas
 - Implica erros de atribuição → Compromete a segurança

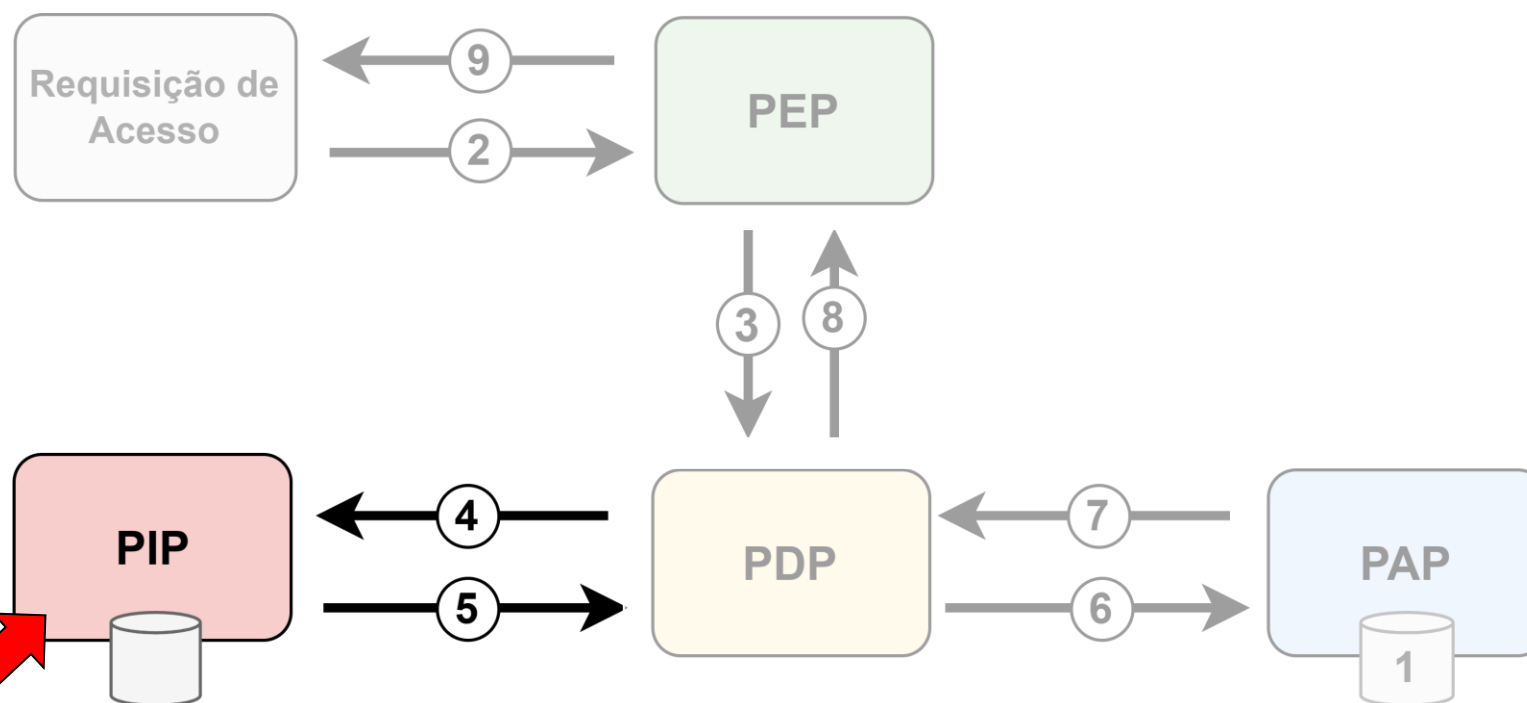
- **PBAC** → Controle de acesso baseado em propósito
 - Relaciona dados com finalidades específicas
 - Aproveita características do **RBAC** e do **ABAC** utilizando tanto papéis quanto atributos
 - Estruturado através de hierarquia
 - Acesso aos dados é concedido mediante verificação do propósito para o qual será usado
 - Relatório, auditoria, nova aplicação, verificação de fraude etc.

- Promove interoperabilidade e terminologia comum para mecanismos de controle de acesso
- Define cinco componentes para lidar com decisões de acesso
 - **PAP** - Policy Administration Point
 - **PEP** - Policy Enforcement Point
 - **PDP** - Policy Decision Point
 - **PIP** - Policy Information Point
 - **CH** - Context Handler



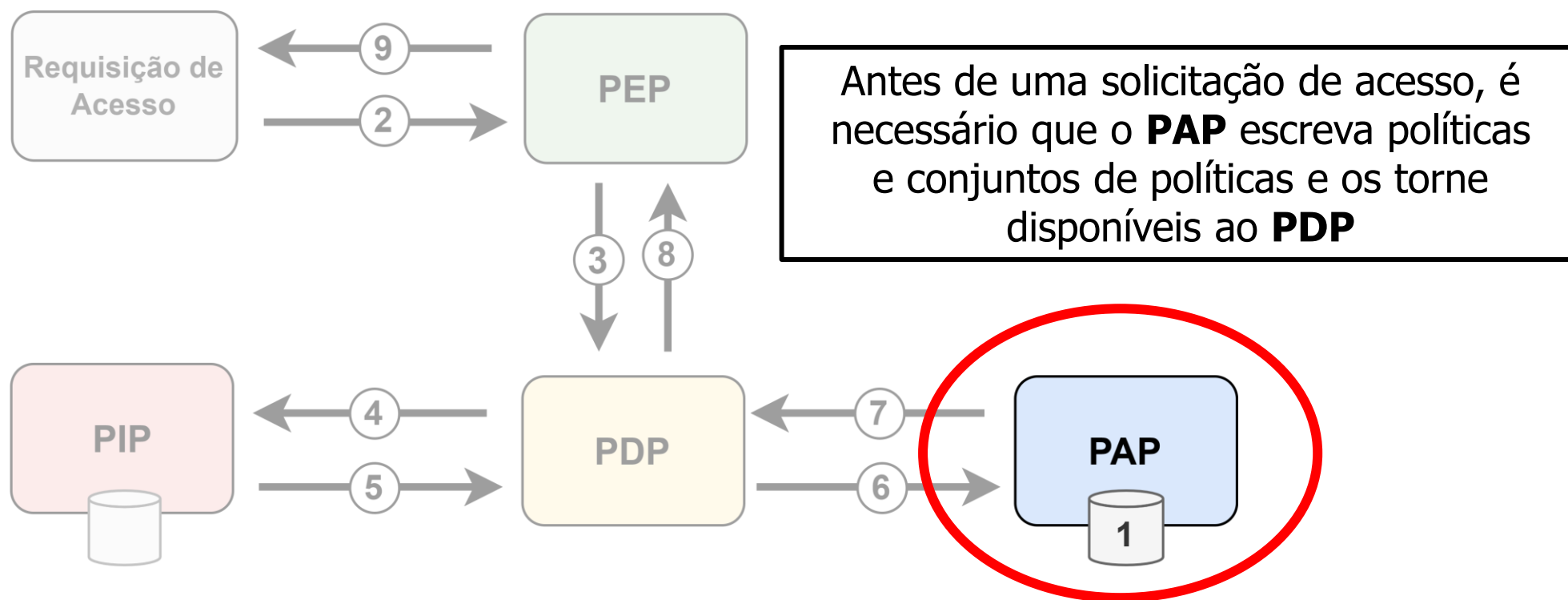


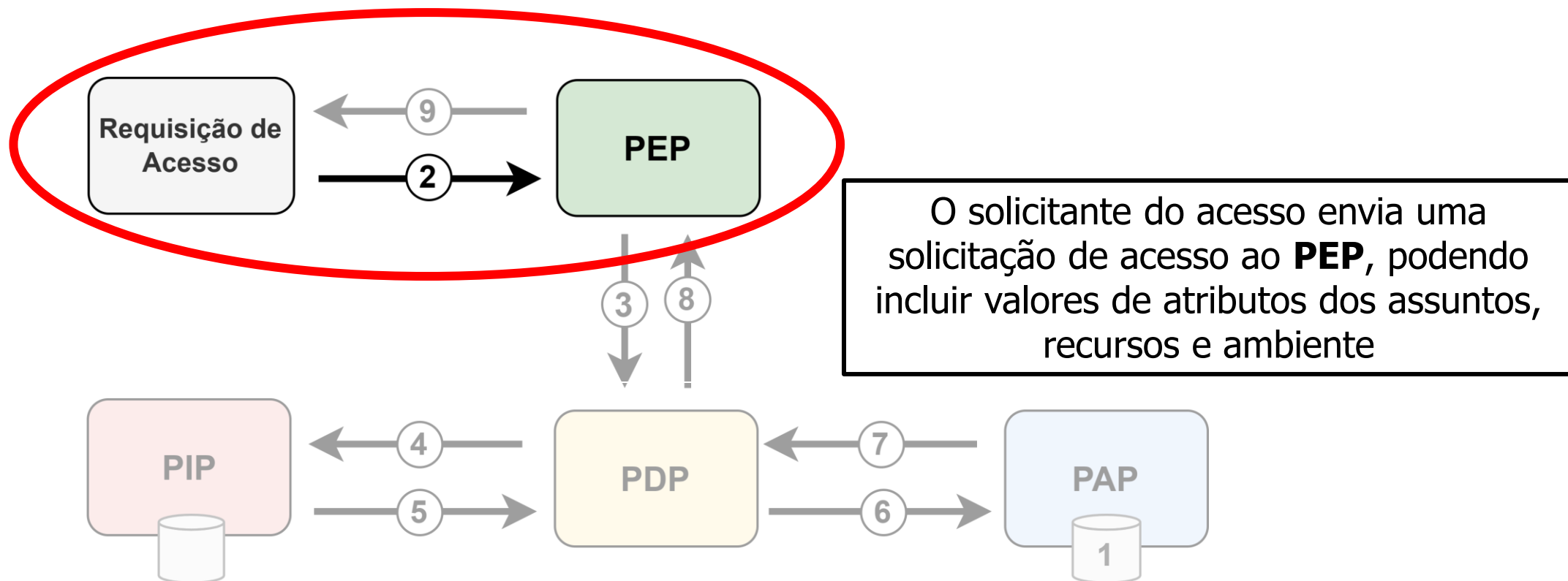


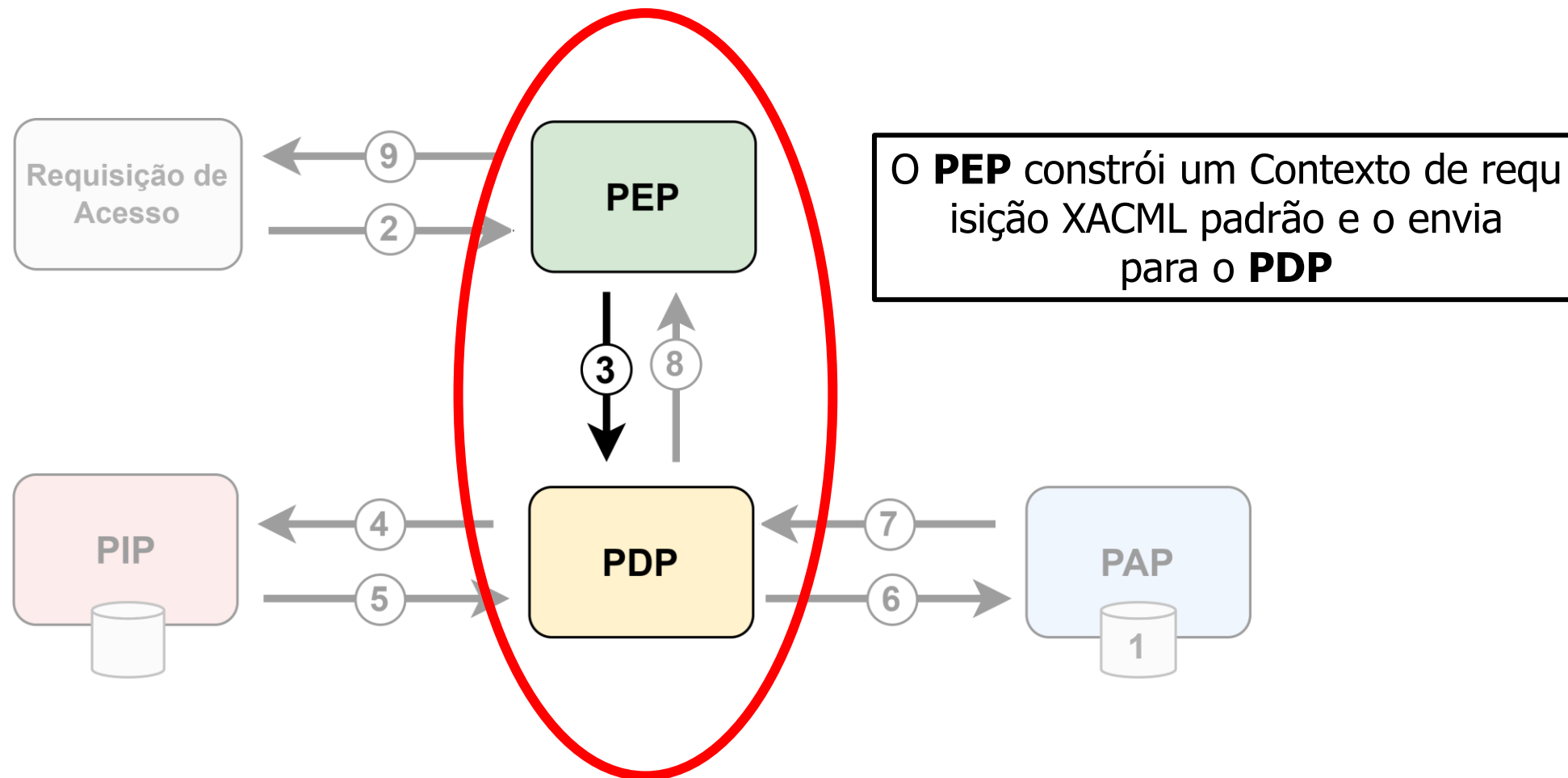


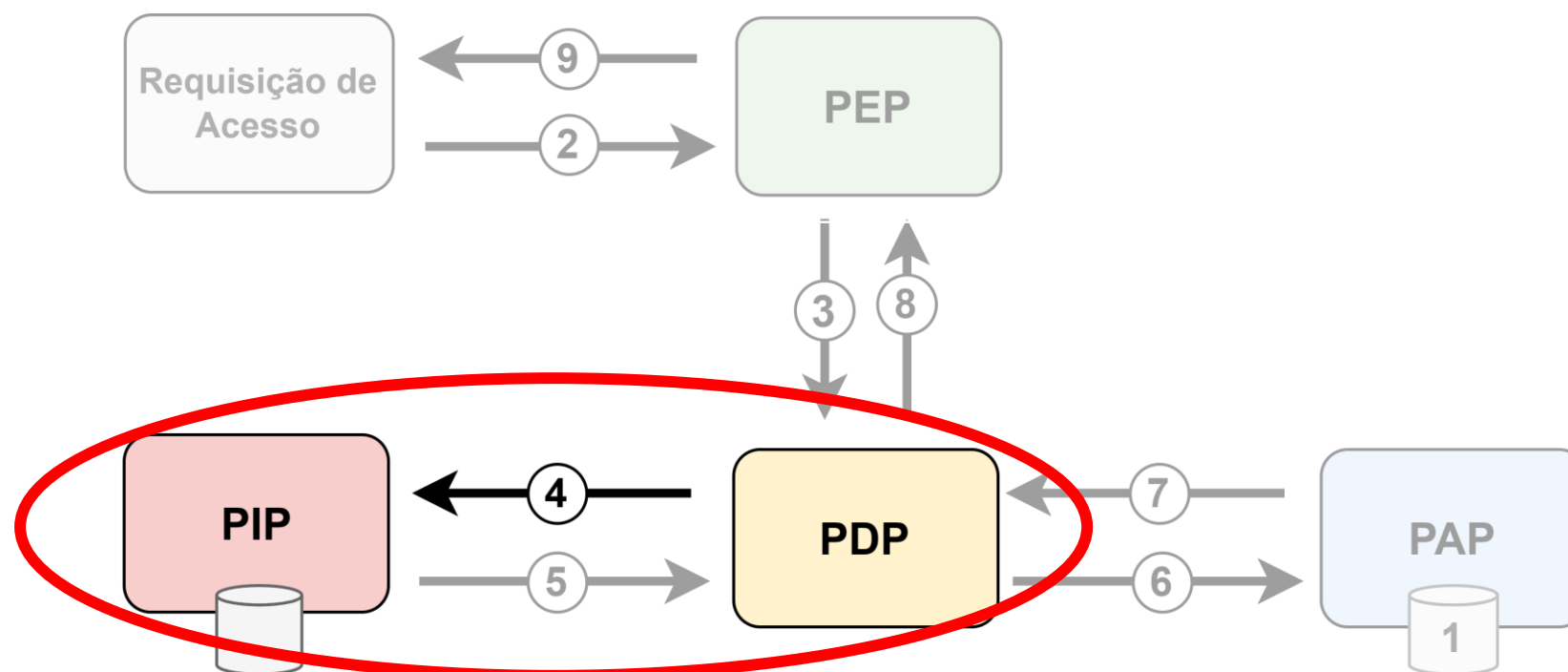
Policy Information Point

Recupera e armazena valores de atributos

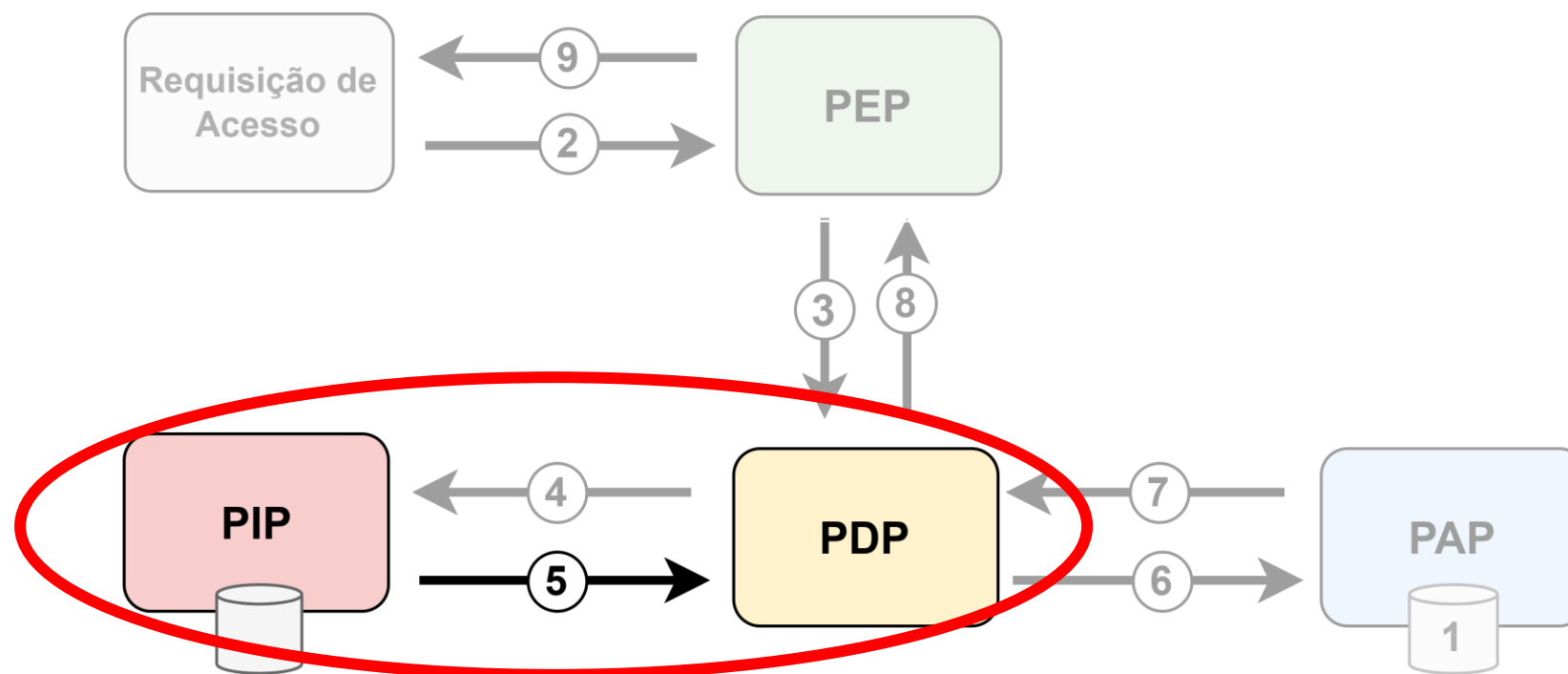




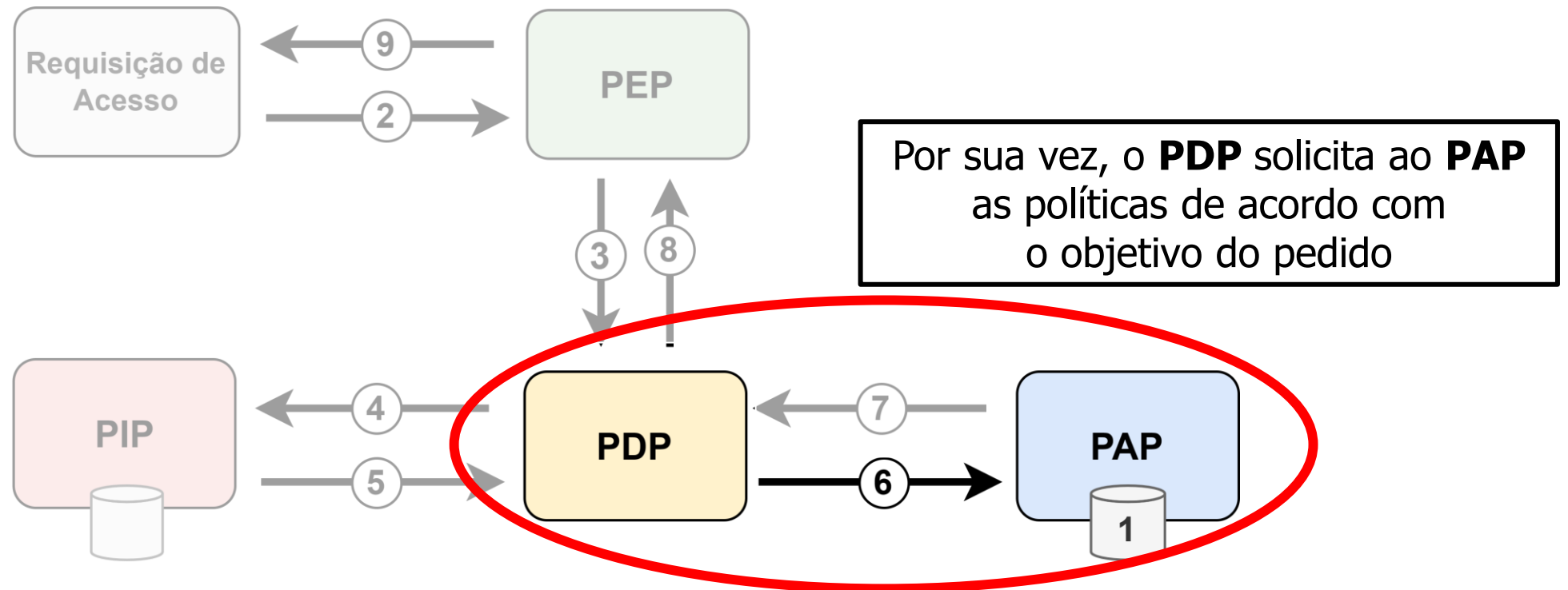


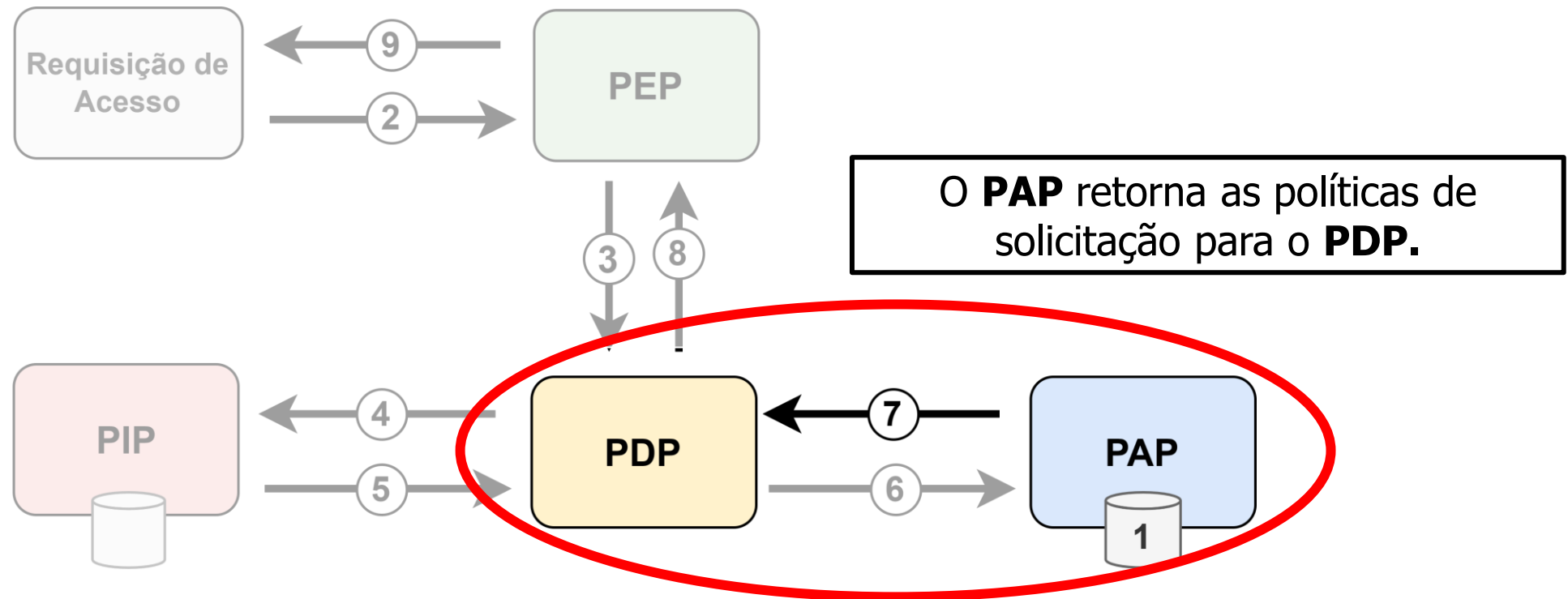


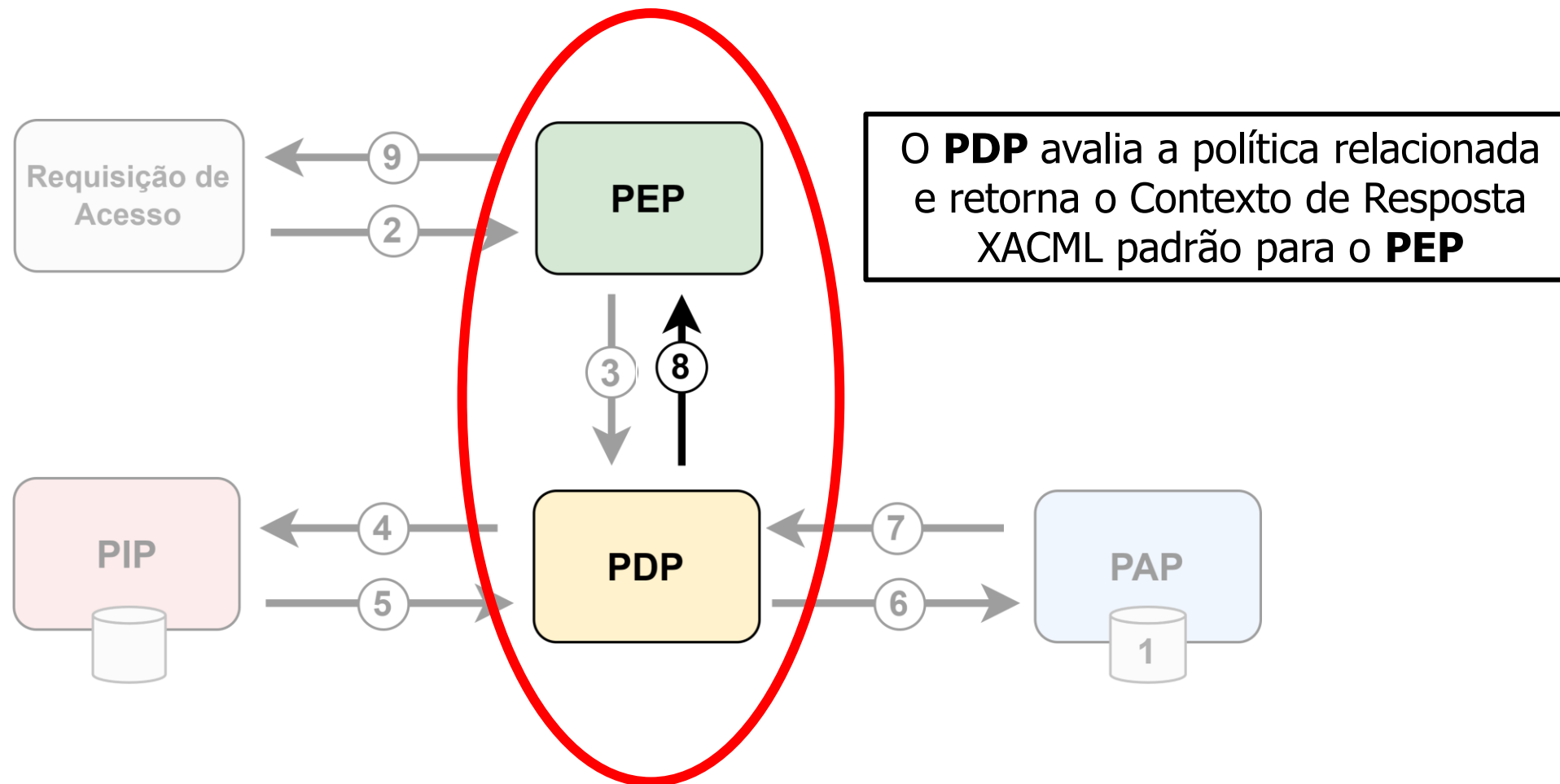
O **PDP** solicita quaisquer valores adicionais de atributo de assunto, de recurso e de ambiente do **PIP**

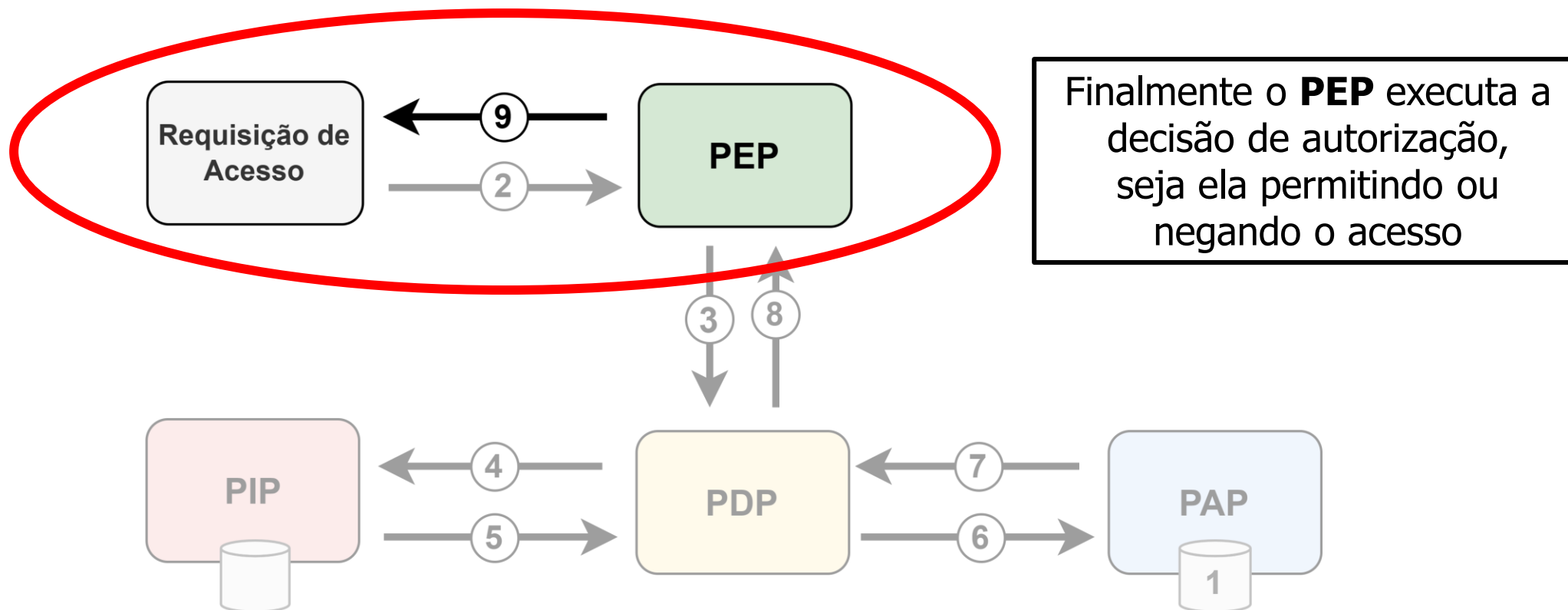


O **PIP** obtém os atributos solicitados e os devolve ao **PDP**









- **GDPR – General Data Protection Regulation**

- Lei vigente desde 2018 em toda a união europeia

- Diretrizes no tratamento para pessoas, empresas ou organização

- Para cumprimento dessa lei no cenário médico, é necessário identificar os **dados sensíveis**

- Uma vez identificados são categorizados de acordo com a sua natureza e sensibilidade

- **GDPR – General Data Protection Regulation**

- Os dados sensíveis ou confidenciais podem ter requisitos específicos
 - Segurança física e lógica
 - Tempo de custódia
 - Criptografia
- No cenário de registros médicos o cenário pode ser mais rígido
 - Ênfase na necessidade de **consentimento** por parte dos pacientes – Descrito no Artigo 7º
 - Uma vez consentido, o controlador deve ser capaz de demonstrar que foi autorizado pelo titular dos dados

- **GDPR – General Data Protection Regulation**

- Uma vez que o consentimento é realizado espontaneamente, um **contrato** está condicionado para processamento dos dados estipulados

- Desafios na geração, manipulação e armazenamento
 - Cenário Híbrido → Contratos impressos e digitais
 - Complexidade na garantia de segurança, principalmente em contratos impressos.
 - Tecnologias utilizando **contratos inteligentes** podem ser consideradas na transição para um **cenário totalmente digital**

- **LGPD – Lei Geral de Proteção de Dados**

- Promulgada em 2018 e similar à GDPR

- Aplicada a qualquer organização que processe dados pessoais em território brasileiro

- **Dados pessoais** → qualquer informação relacionada a uma pessoa natural ou pessoa jurídica, de direito público ou privado

- Informações pessoais

- Nome, endereço, e-mail, número de identidade, entre outros

- **LGPD – Lei Geral de Proteção de Dados**

- Agentes de tratamento

- Pessoa natural ou jurídica que realize **qualquer** operação sobre os dados pessoais de outrem
 - Deveres → Coleta de consentimento explícito do titular dos dados e produção de relatórios que identifiquem as operações de tratamento aos dados

- Violações nos dados devem ser reportados à ANPD (Autoridade Nacional de Proteção de Dados)

- **LGPD – Lei Geral de Proteção de Dados**

- Dados de saúde são considerados **dados pessoais sensíveis**

- Exige-se o consentimento por parte do titular através do **Termo de Consentimento Livro e Esclarecido (TCLE)**

- Documento complementar com objetivo de esclarecer dúvidas acerca de intercorrências, riscos envolvidos ou outras informações sobre tratamento ou procedimento médico
 - Normalmente preenchido e assinado manualmente → Dificuldade em manter sigilo

- **LGPD – Lei Geral de Proteção de Dados**

- Tenta abranger o maior número possível de casos

- Cenários em que existem documentos impressos são desafiadores

- Sistemas informatizados são custosos

- Falta de infraestrutura, principalmente em áreas rurais, dificulta o acesso a dados digitalizados

- Lei é abrangente e não existe lei específica nem complementar acerca de dados de saúde, diferentemente dos Estados Unidos

- **HIPPA – Health Insurance Portability and Accountability**

- Lei americana, criada em 1996, **específica** para proteção de informações de saúde
- Estabelece padrões de privacidade e segurança para informações médicas, conhecidas como **PHI – Protected Health Information**
 - Restringe o acesso e divulgação dos dados
- Define diretrizes de privacidade relacionadas aos direitos e limites de privacidade dos pacientes
 - Compreender e controlar os dados

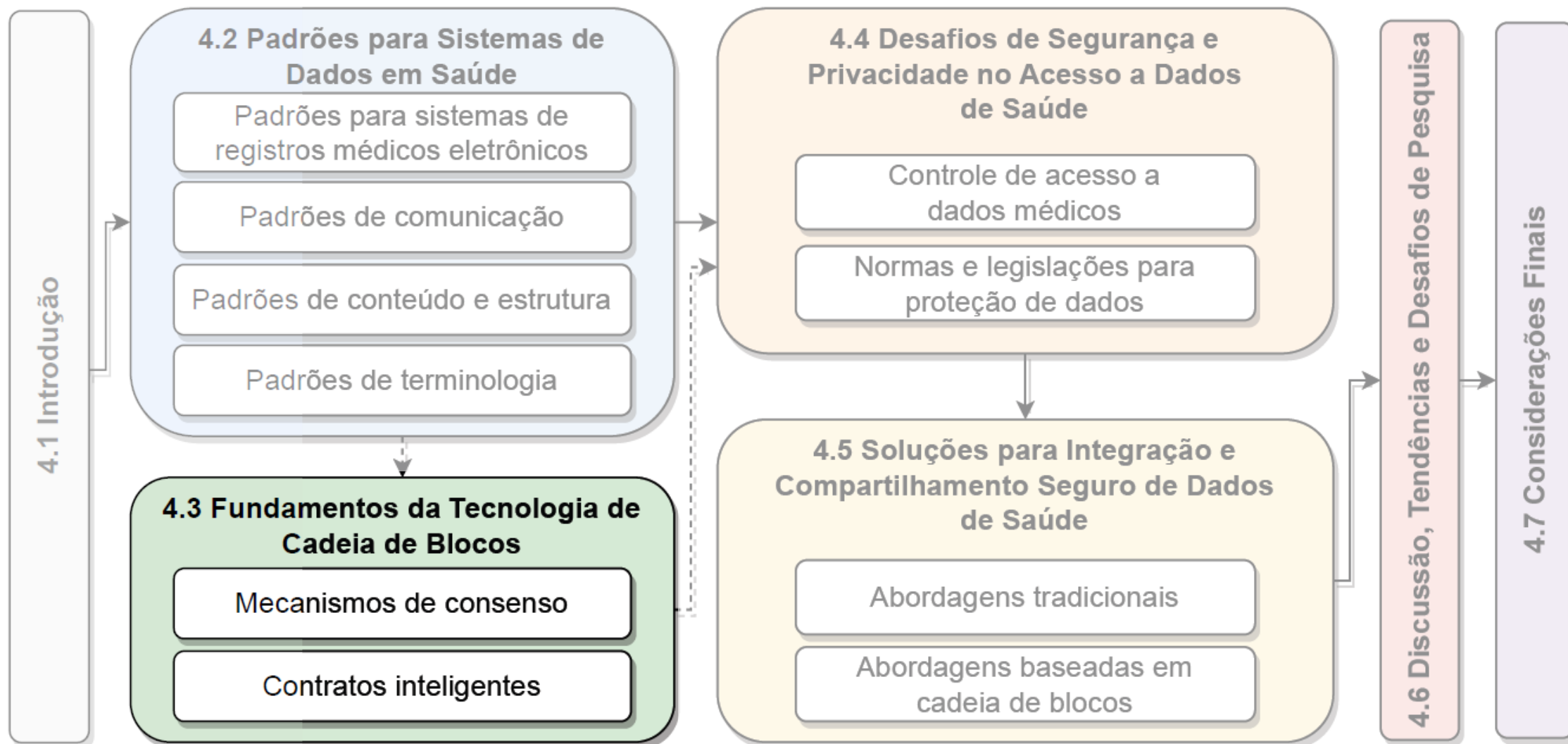
- **HIPPA – Health Insurance Portability and Accountability**

- 7 termos principais

- **Compreensão dos pacientes** → pacientes têm direito de compreender os processos envolvidos no tratamento dos seus dados
- **Confidencialidade** → dados devem ser protegidos em todas as etapas
- **Controle dos pacientes** → pacientes devem ser capazes de controlar e autorizar quem pode acessar e utilizar seus dados de saúde
- **Integridade dos dados** → dados dos pacientes devem ser protegidos contra modificações ou destruição não autorizadas
- **Exceção de consentimento** → dados de saúde podem ser divulgados e usados sem a autorização individual do paciente em casos de risco à vida
- **Não repúdio** → quaisquer atividades relevantes devem ser apoiadas por evidências verificáveis
- **Auditoria** → pacientes devem receber garantias quanto à segurança e proteção de seus dados

- **HIPPA – Health Insurance Portability and Accountability**
 - Projetada para que seja flexível e abrangente
 - Possui mecanismos para casos de violações de informações de saúde
 - Ocorre através do uso ou divulgação não autorizada sob a "**Regra de Privacidade**"
 - Estipula padrões para proteção dos registros médicos dos indivíduos e outras informações de saúde
 - Existem três exceções no que diz respeito à definição de violação
 - Aquisição, acesso ou uso não intencional de informações protegidas
 - Divulgação inadvertida de informações protegidas
 - Se entidade coberta (planos de saúde, hospitais e clínicas) acreditar de boa-fé, para quem o dado foi disponibilizado, não seria capaz de reter informações

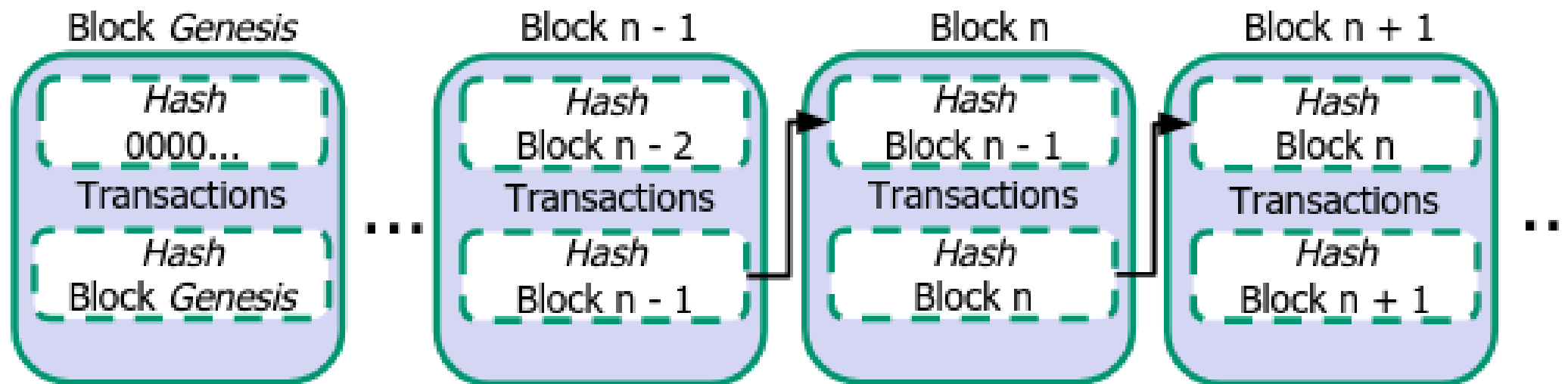
Roteiro do Minicurso



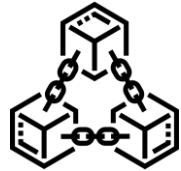
Cadeia de Blocos

Definição Formal

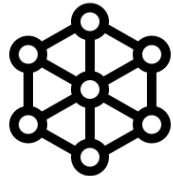
"Tecnologia de livro razão distribuído que permite que qualquer participante na rede de negócios leia o registro único gravado (o livro razão – ledger)"



- **Cadeia de Blocos** A.K.A. *Blockchain*
 - **Composição**



Estrutura de dados de encadeamento dos blocos



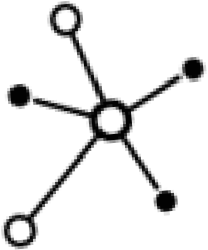
Rede par-a-par

- capaz de armazenar transações de forma ordenada e distribuída

- **Diferencial**

- Desenvolvimento de **aplicações distribuídas seguras**
 - Mesmo em cenários marcados pela desconfiança mútua entre entidades
- Dispensa a necessidade de uma **terceira entidade centralizadora**
 - Atua como âncora de confiança → assegurando a segurança entre transações na rede

Descentralização



- Não há necessidade de **intermediário**
- O sistema de banco de dados está **disponível globalmente** na rede
 - Para qualquer usuário com nível de acesso necessário
- **Monitoramento, armazenamento, acesso e atualização de dados** podem ser realizados nos diversos sistemas que fazem parte da rede



Transparência

- Dados registrados e armazenados são transparentes para os usuários
 - **Todos os usuários podem visualizar as transações** realizadas via *blockchain*



Imutabilidade

- Dados armazenados **não podem ser adulterados facilmente**
 - Pode-se provar com certeza matemática que o fluxo de dados históricos é exato



Autonomia

- Cada nó da rede é **independente e autônomo**
 - Podendo acessar, transferir, armazenar e atualizar dados com segurança e sem intervenção externa

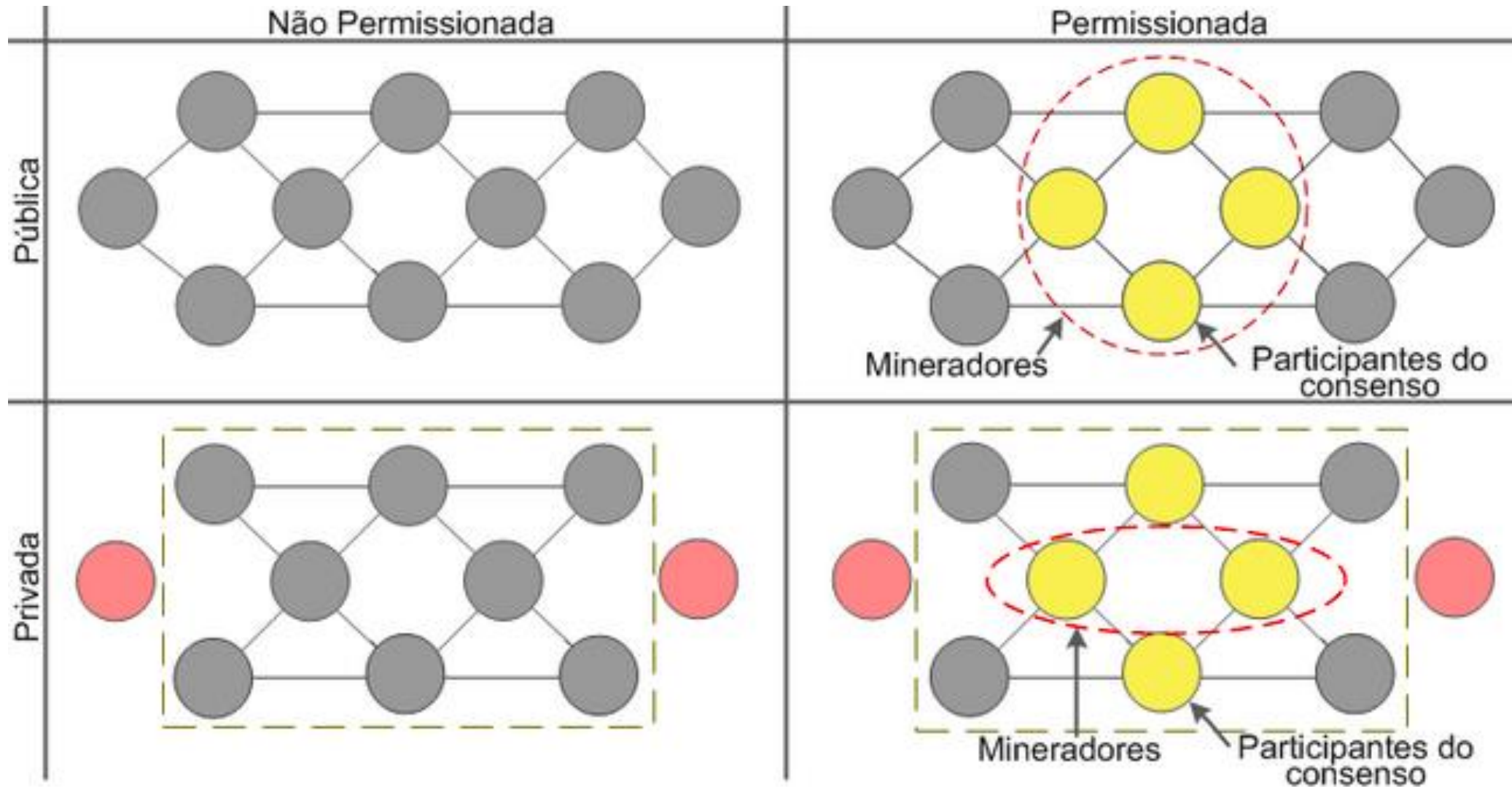


Anonimato

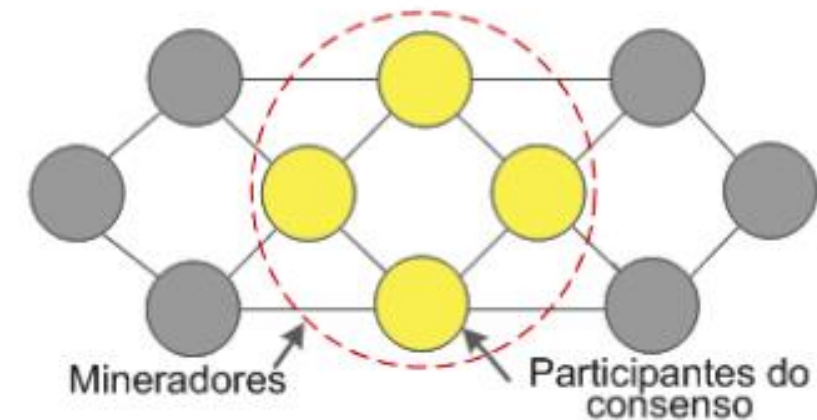
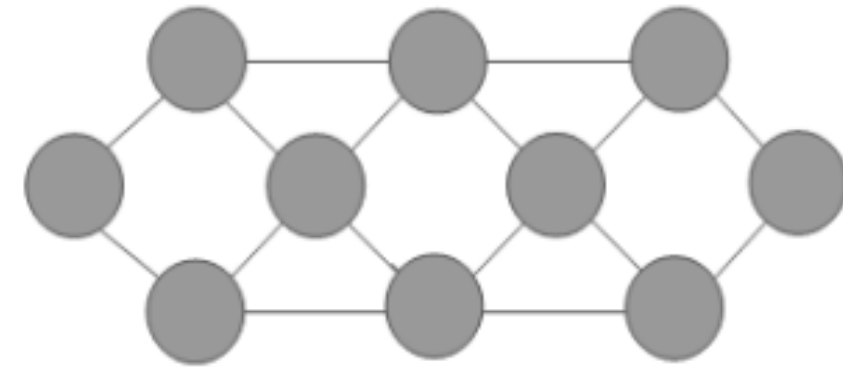
- **Preservação da identidade** dos participantes
 - Contribuindo para a privacidade, segurança e confiabilidade do sistema

Cadeia de Blocos

Taxonomia



- **Redes Públicas Não Permissionadas**
 - Ausência de controle de acesso
 - Todos os nós podem ser mineradores
 - Exigência de mecanismos de consenso mais robustos
 - Ex: Bitcoin, Ethereum
- **Redes Públicas Permissionadas**
 - Ausência de controle de acesso
 - Nós mineradores têm permissões para...
 - Gerar blocos
 - Participarem do consenso



- **Redes Privadas Não Permissionadas**

- Existência de controle de acesso
- Todos os nós são iguais na rede
- Ex:



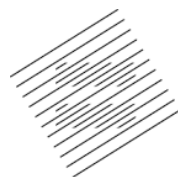
- **Redes Privadas Permissionadas**

- Existência de controle de acesso
- Nós mineradores têm permissões para...
- Gerar blocos e
- Participarem do consenso

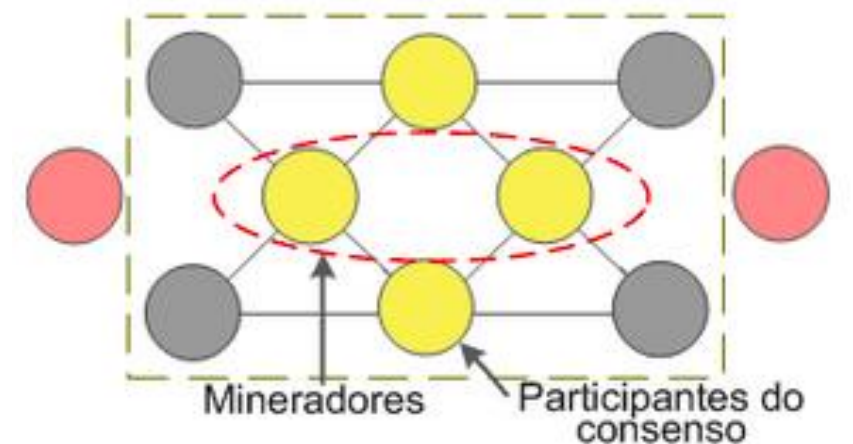
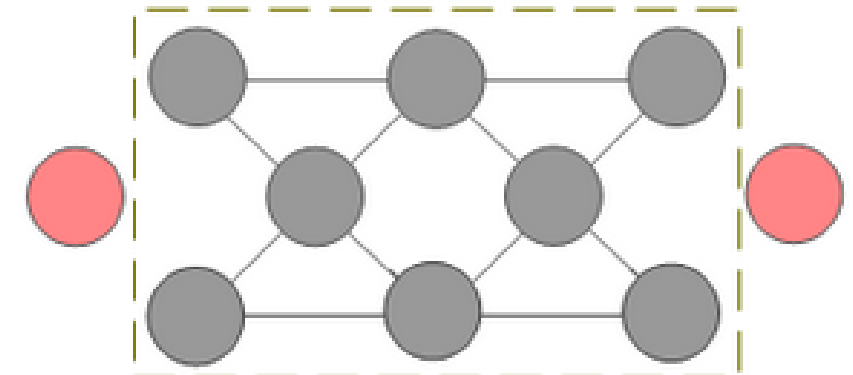
– Ex:



MultiChain



parity

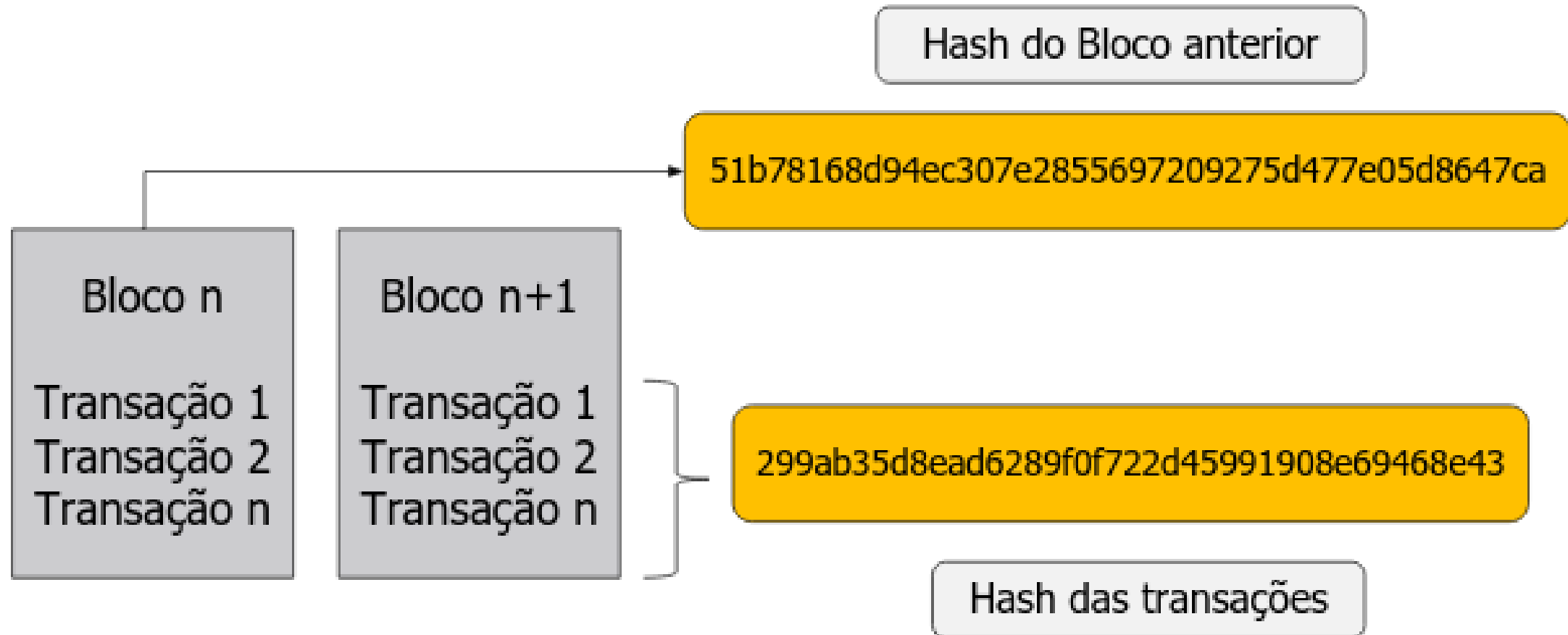


Cadeia de Blocos

Mecanismos de Consenso

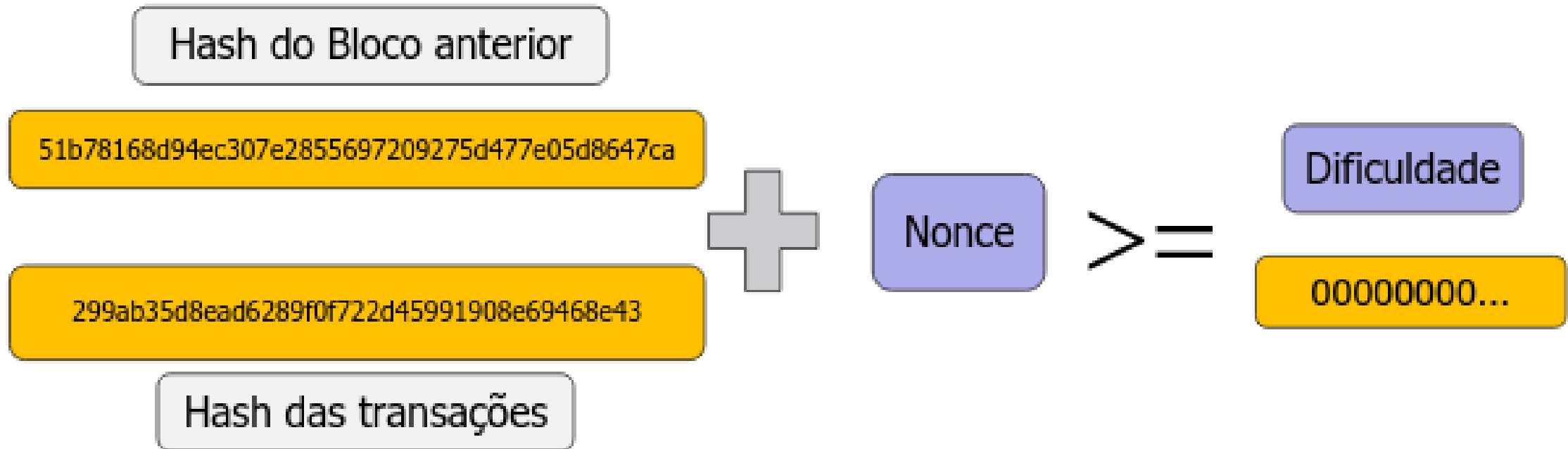
- **Descentralização das Cadeias de Blocos** → impede a existência de um ponto único de falha
 - Fato que **prejudicaria a segurança e a privacidade das transações** realizadas
 - Nós participantes da rede par-a-par acessam uma **réplica idêntica da cadeia de blocos**
 - Replicação armazenada localmente
- **Implicações**
 - Adoção de **mecanismos de validação e de consenso**
 - Para evitar inconsistências e garantir a distribuição de réplicas coerentes dos dados
- **Exemplos de Protocolos de Consenso**
 - Prova de Trabalho
 - Prova de Participação
 - Prova de Autoridade
 - Protocolos de Consenso Baseados em Votação
 - Raft

- **Prova de Trabalho** A.K.A *Proof-of-Work* (PoW)
 - Mecanismo de consenso probabilístico
 - **Princípio de Funcionamento**
 - Baseado na competição entre mineradores
 - Nós buscam resolver um desafio criptográfico difícil → através de **força bruta**
- Assim...*
- O primeiro nó minerador a resolver o desafio
 - Encontra um valor número aleatório → **nonce**
 - Gravado no cabeçalho do bloco, juntamente com o hash do bloco anterior
 - *Nonce* relaciona-se ao número esperado de zeros iniciais do hash do bloco
 - Recebe uma recompensa pelo esforço
- Logo...*
- Quanto **maior o poder computacional** do nó
 - Maior a probabilidade do nó minerar um bloco



Mecanismos de Consenso em Cadeias de Blocos

Prova de Trabalho



Cadeia de Blocos

Mecanismos de Consenso

- **Prova de Participação** A.K.A *Proof-of-Stake* (PoS)
 - Mecanismo de consenso probabilístico
 - **Princípio de Funcionamento**
 - Também baseado na competição entre mineradores
 - Porém a **probab. de sucesso na mineração depende da participação dos nós** na rede
- Assim...
- Mineradores precisam encontrar um valor de *hash* menor ou igual a um valor alvo
 - A dificuldade para encontrar esse *hash* é
 - Inversamente proporcional à **riqueza acumulada** (*coin age*) daquele nó



quantidade de recursos do nó multiplicada pelo **período em que o nó reteve aquele recurso**

Logo...

- Quanto maior a participação e riqueza acumulada de um nó
 - Maior a probabilidade deste nó validar o próximo bloco

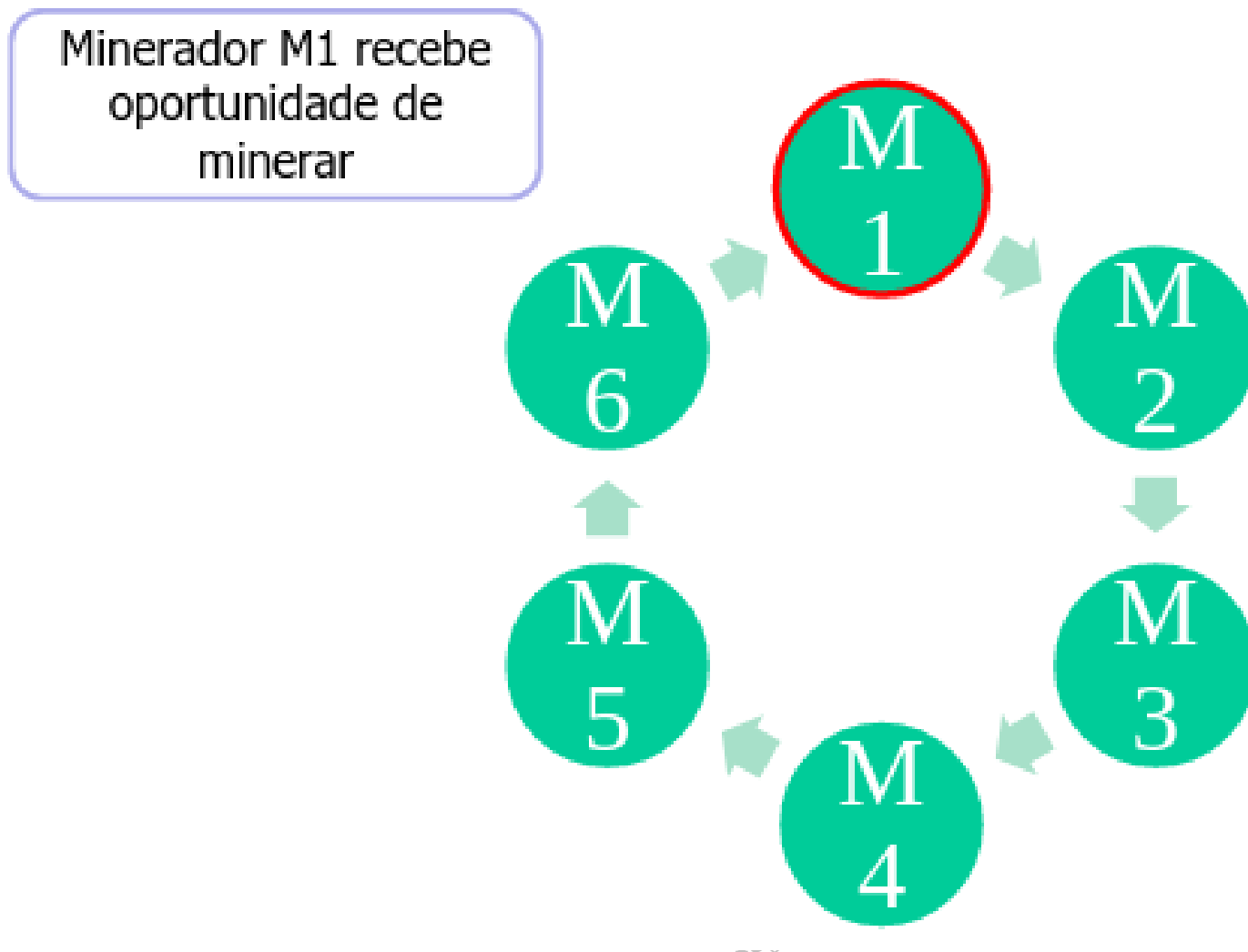
Cadeia de Blocos

Mecanismos de Consenso

- **Prova de Autoridade** A.K.A *Proof-of-Authority* (PoA)
 - Mecanismo de consenso probabilístico
 - Amplamente adotado em redes privadas
 - **Princípio de Funcionamento**
 - Baseado na presença de um conjunto de **nós com autoridade**
 - Encarregados da tarefa de gerar novos blocos e validar as transações
 - Designados por uma entidade
- Assim...*
- **Antes da inclusão de qualquer bloco** candidato na cadeia
 - Cada bloco é validado e assinado por pelo menos um nó com autoridade
 - Para evitar disputas e desperdícios de recursos
 - Aplicação de um esquema rotativo de geração de blocos
 - Alocando um intervalo de tempo exclusivo a cada nó de autoridade
- **Manutenção da Natureza Distribuída**
 - Garantida pela concordância unânime entre os nós de autoridade sobre o estado global da cadeia

Mecanismos de Consenso em Cadeias de Blocos

Prova de Autoridade - Funcionamento

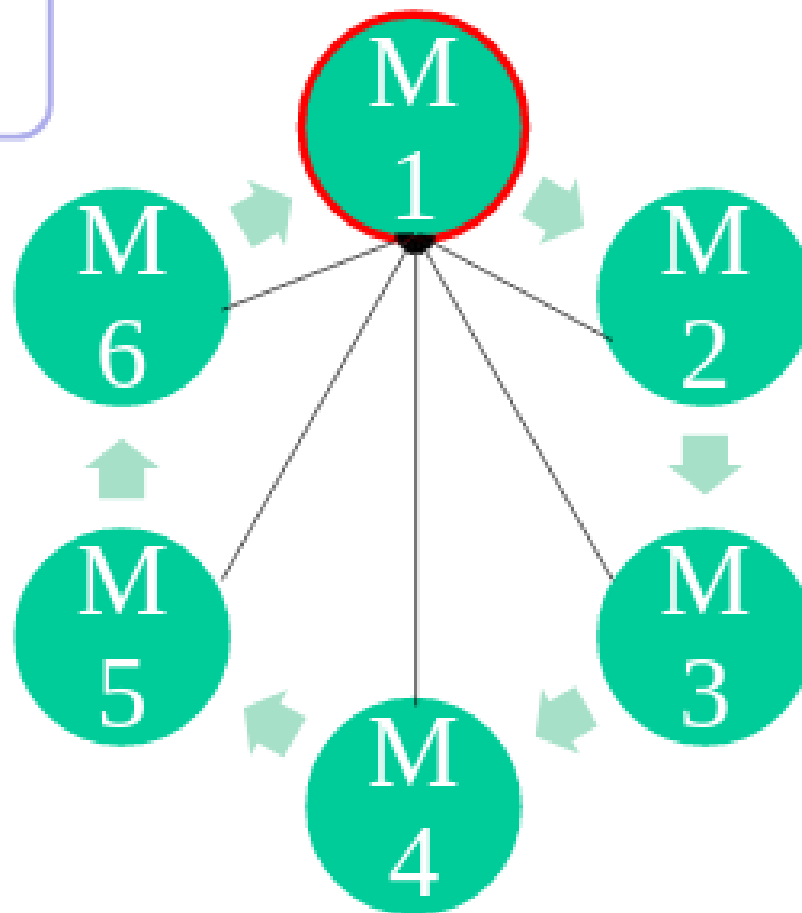


Mecanismos de Consenso em Cadeias de Blocos

Prova de Autoridade - Funcionamento

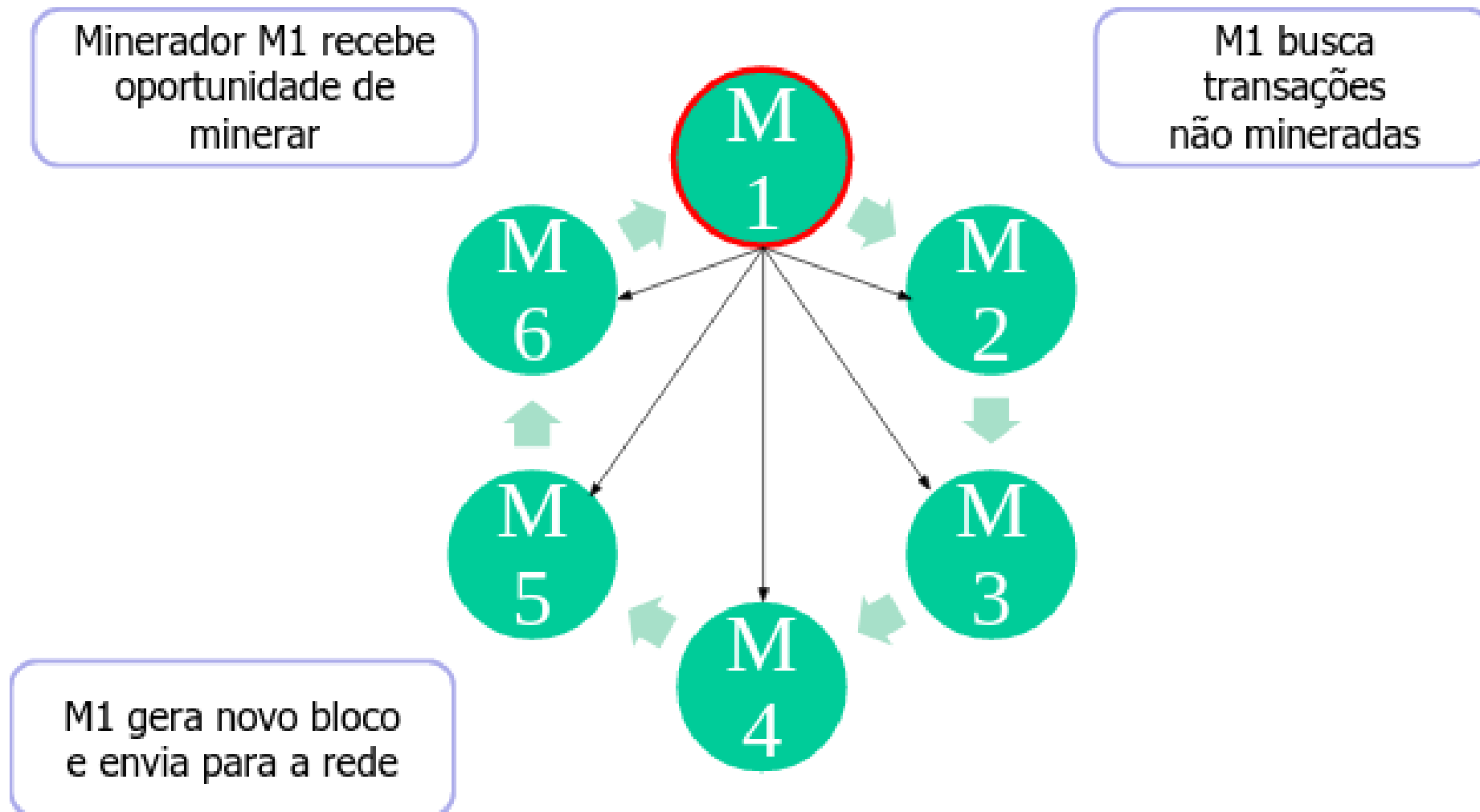
Minerador M1 recebe
oportunidade de
minerar

M1 busca
transações
não mineradas



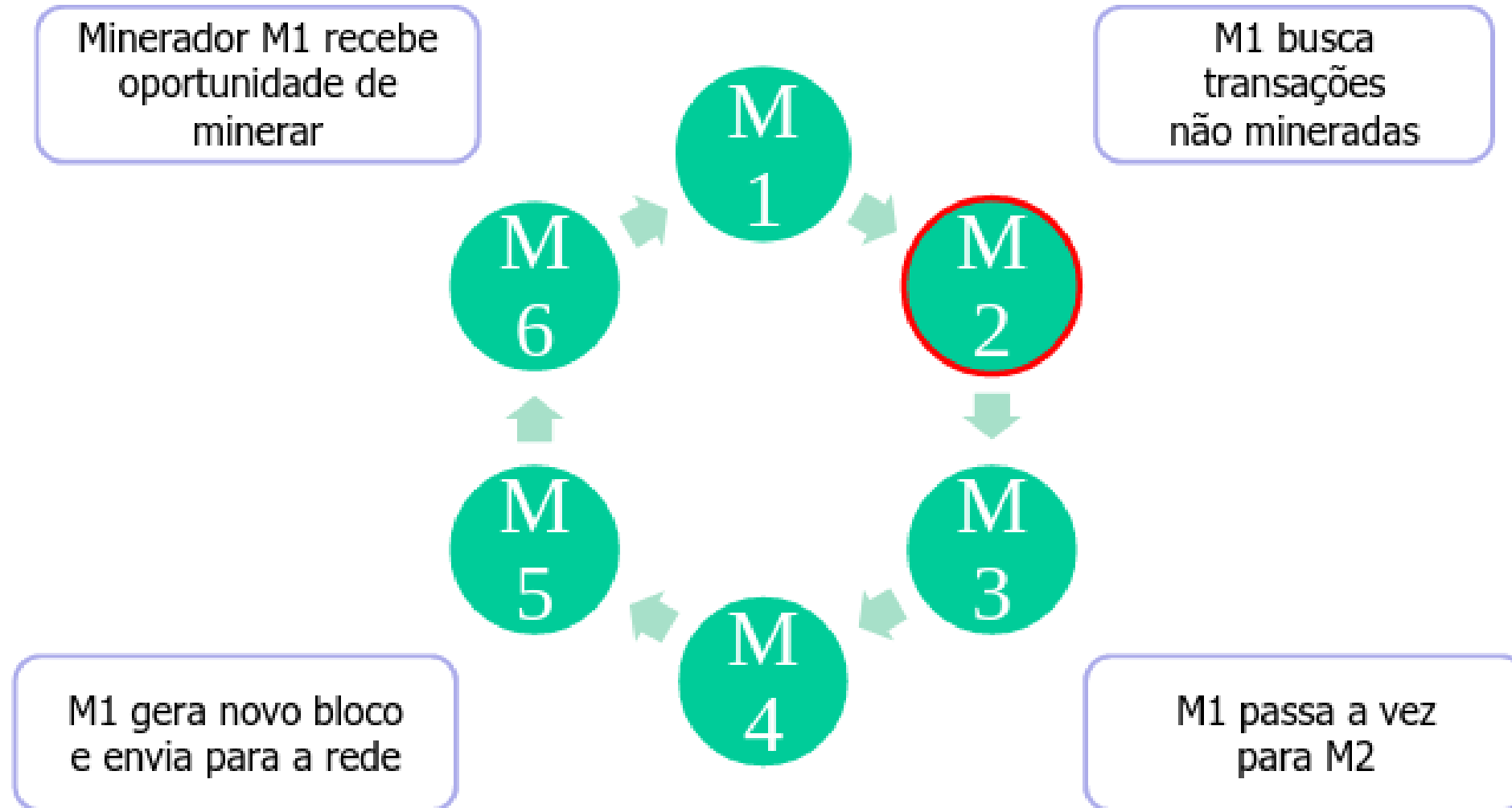
Mecanismos de Consenso em Cadeias de Blocos

Prova de Autoridade - Funcionamento



Mecanismos de Consenso em Cadeias de Blocos

Prova de Autoridade - Funcionamento



Cadeia de Blocos

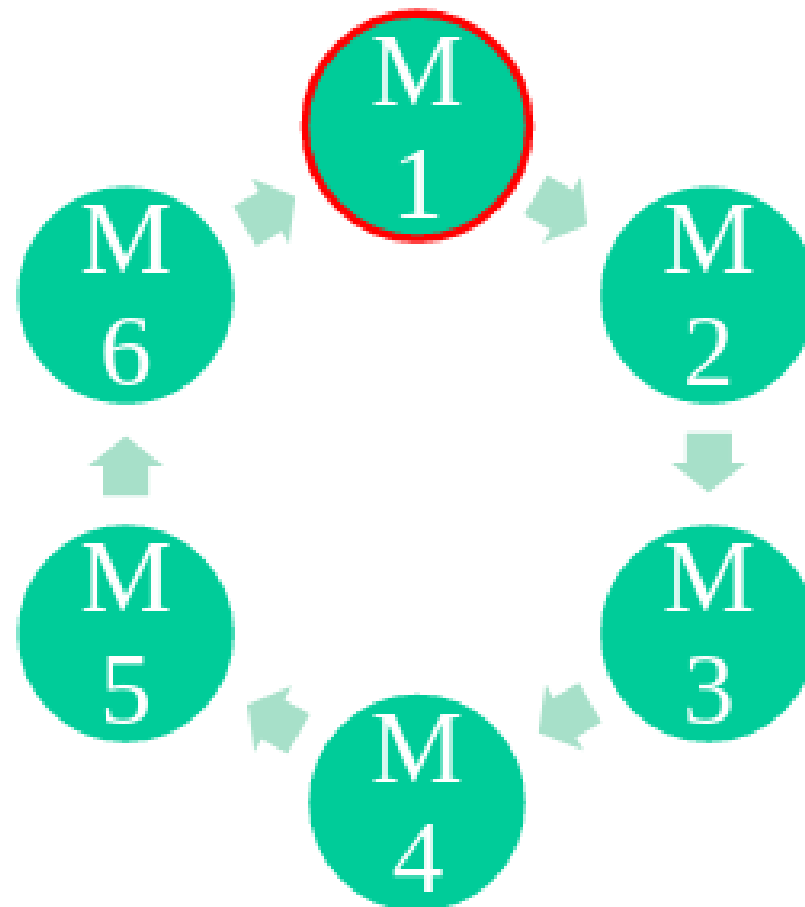
Mecanismos de Consenso

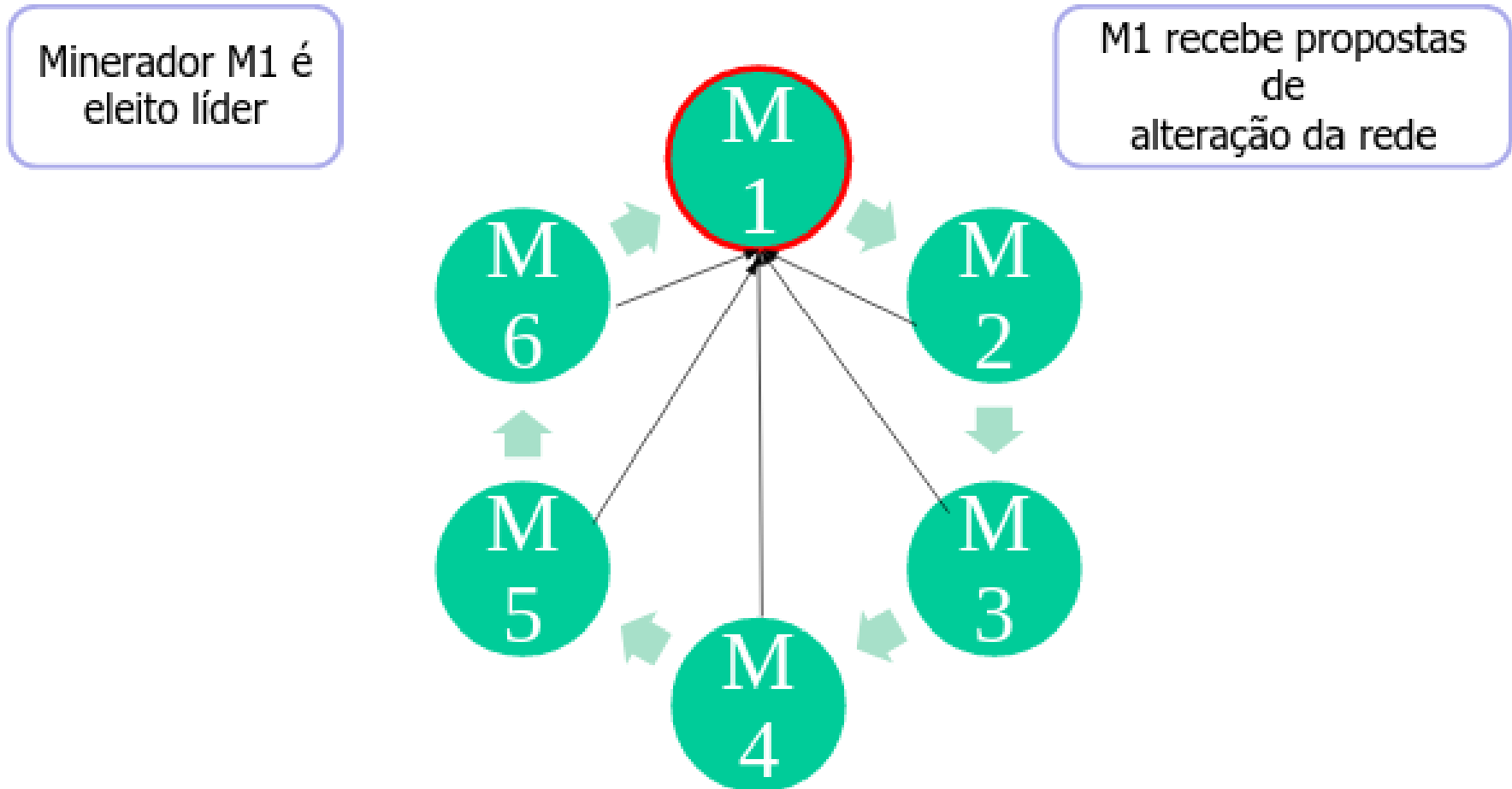
- **Raft** → Mecanismo de consenso tolerante a falhas
 - Usado na plataforma Hyperledger Fabric
 - Recomendado para ambientes de produção
- **Princípio de Funcionamento**
 - Baseado na baseado no **modelo líder-seguidor**
 - Em que cada nó pode assumir **3 estados:** *Candidato ou seguidor ou líder*
 - *O consenso é...*
 - Alcançado por meio da eleição de um líder, replicação de log e estágios de segurança
- **Vantagens**
 - Fácil implementação em linguagens de programação mais comuns
 - Adota um sistema de eleição eficiente
- **Desvantagens**
 - Requer capacidade de armazenamento significativa
 - Ausência de tratamento de falhas Bizantinas
 - Comportamento de um nó que foge ao comportamento esperado do protocolo definido

Mecanismos de Consenso em Cadeias de Blocos

Raft - Funcionamento

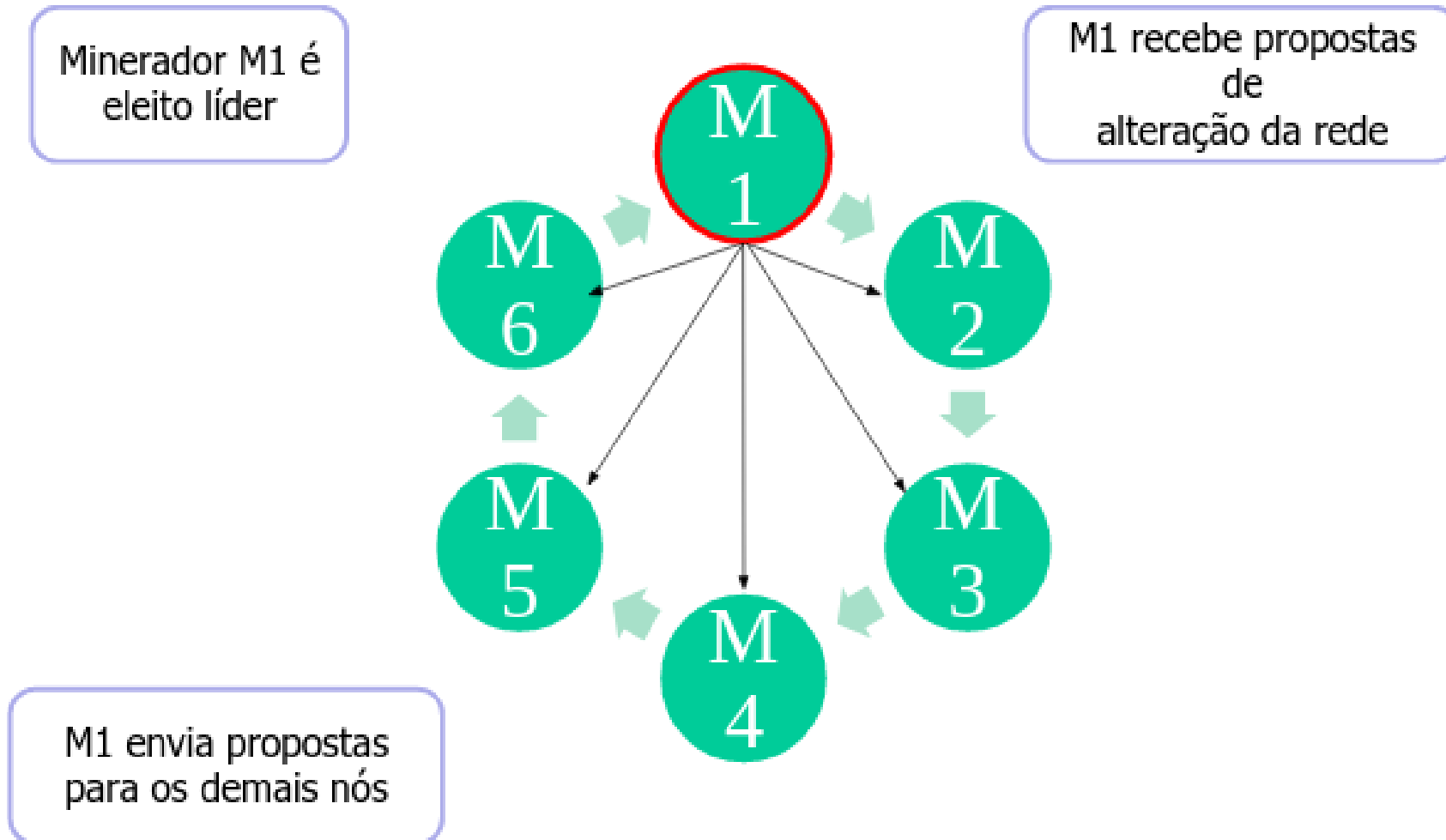
Minerador M1 é
eleito líder

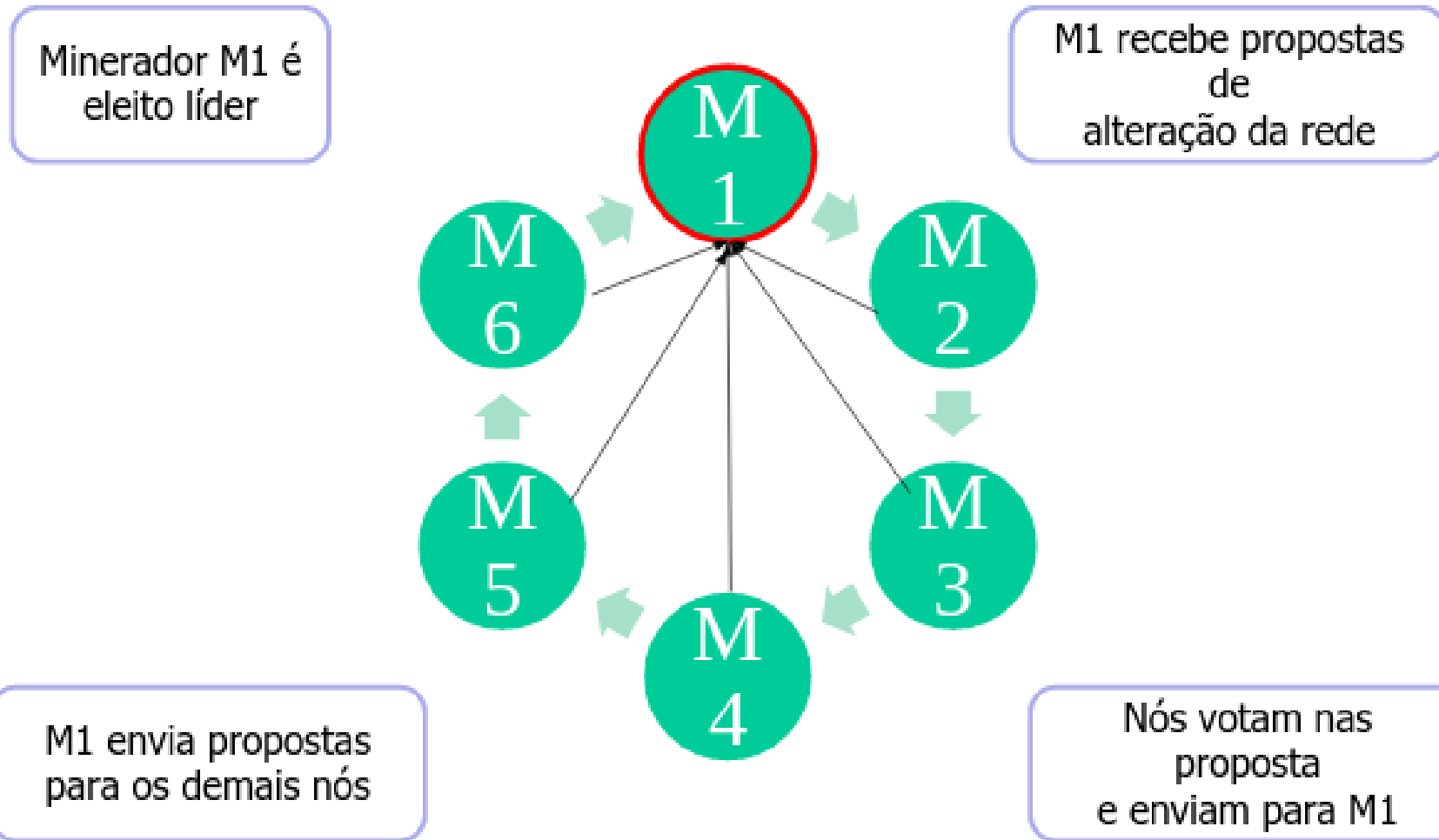




Mecanismos de Consenso em Cadeias de Blocos

Raft - Funcionamento





- **Contratos Inteligentes** A.K.A. *smart Contracts*
 - Introduzido na plataforma de computação confiável Ethereum
 - Consiste em uma **aplicação autoexecutável armazenada na cadeia de blocos**
 - **Função Geral**
 - Traduzir cláusulas de um contrato real para código



Contrato Tradicional

- Escrito em **linguagem natural**
 - Jurídica
- Execução pelos participantes
- Registro em cartório



Contratos Inteligentes

- Escrito em **linguagem script**
- Auto-executável
 - decisões baseadas nos dados de entrada
- **Registro na cadeia de blocos --> inspecionável**

Cadeias de Blocos

Usabilidade Área de Saúde

- *Blockchain* → **Naturalmente atrativa no âmbito de saúde**
 - **Por quê?**
 - Auxilia na **padronização e interoperabilidade** de EMRs
 - **Como?**
 - Permite que o EMR seja **verificado e registrado** por meio de um consenso de pares
 - **Benefícios**
 - Garantia da execução confiável de políticas de acesso aos dados; e
 - Assegurando a **integridade** dos dados, **responsabilidade** e **não repúdio**



Igualmente interessante no...

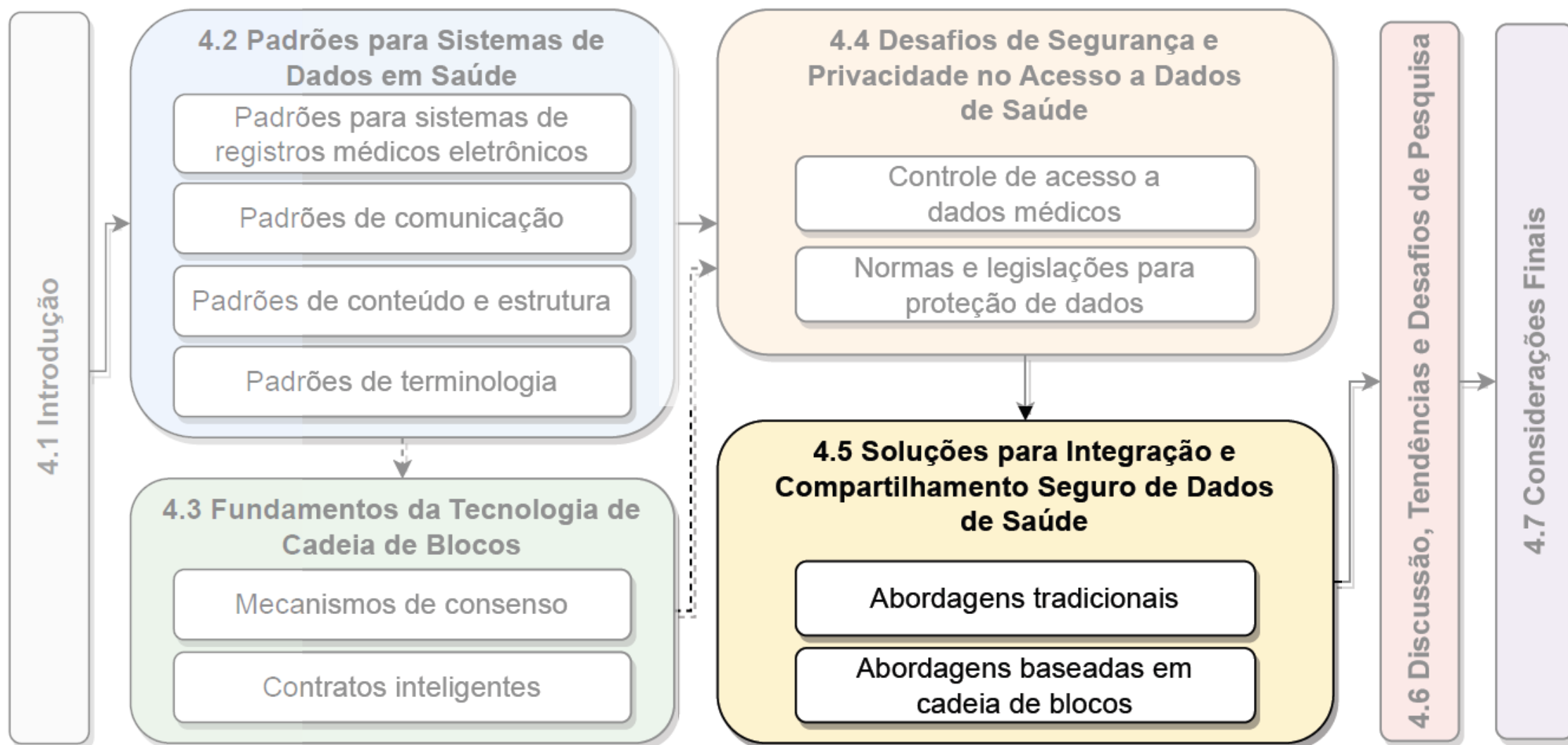
- Desenvolvimento de aplicações que
 - (i) exigem a **contribuição de várias partes interessadas**
 - embora a garantia de confiança entre as partes seja complexa atualmente
 - (ii) carecem de um **rastreamento confiável** de atividade e **confiabilidade** de dados e
 - (iii) desejam **remover partes intermediárias** → aumentando a eficiência geral do sistema

O QUE VIMOS ATÉ AQUI...

- Sistemas Médicos Tradicionais
- Registros Médicos Eletrônicos
 - Definição, problemas, e desafios
- Padrões para Dados de Saúde
 - Padrões de sistemas de registros médicos eletrônicos: openEHR
 - Padrões de comunicação: FHIR, DICOM
 - Padrões de conteúdo e estrutura: C-CDA, HL7 V2 e V3
 - Padrões de vocabulários: TUSS, LOINC, SNOMED e ICDx

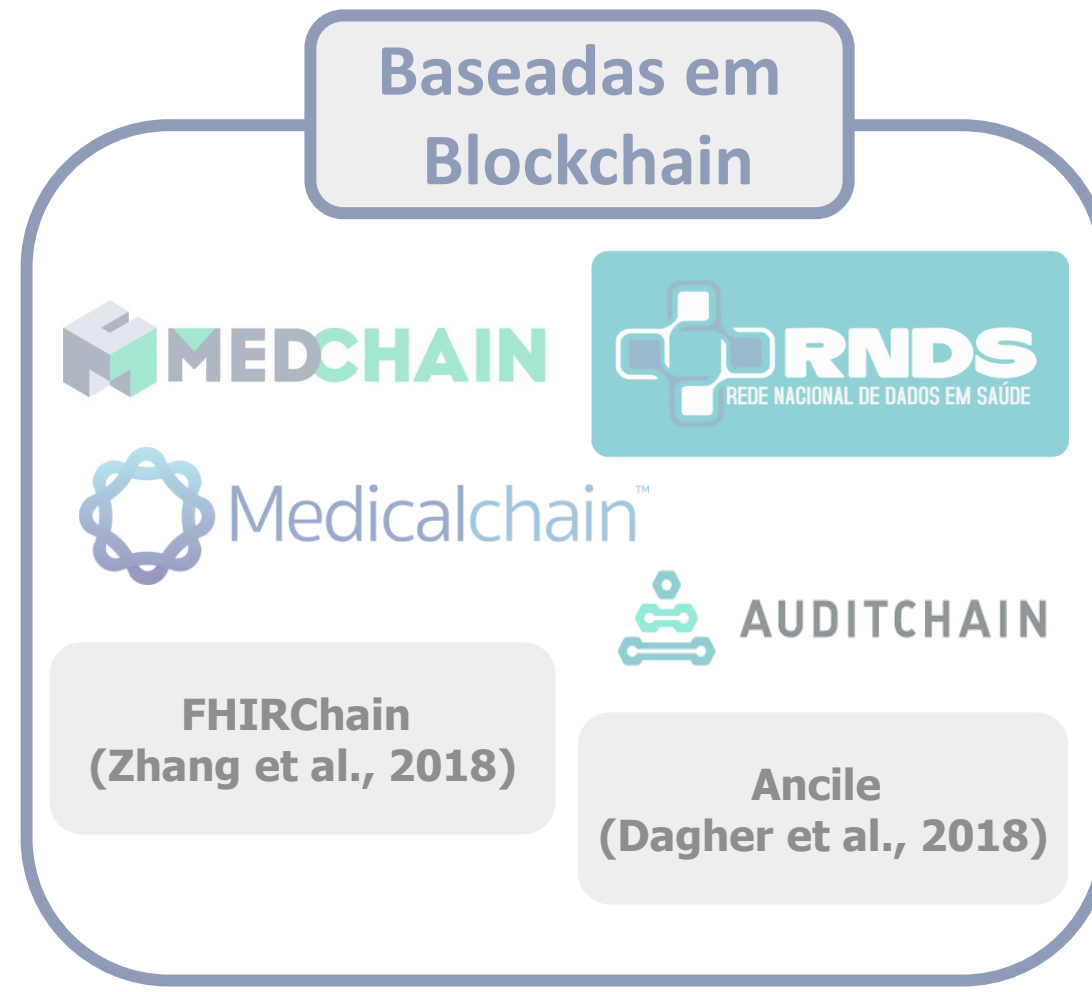
- **Desafios de Segurança e Privacidade no Acesso a Dados de Saúde**
 - Mecanismos de Controle de Acesso a Dados Médicos
 - RBAC, ABAC, PBAC, SitBAC
 - Normas e Legislações para Proteção de Dados
 - LGPD, GDPR e HIPAA
- **Fundamentos de Cadeias de Blocos**
 - Definição e Propriedades e Taxonomia
 - Protocolos de Consenso

Roteiro do Minicurso



Soluções de Integração e Compartilhamento

Abordagens Tradicionais



Abordagens Tradicionais

AGHUX



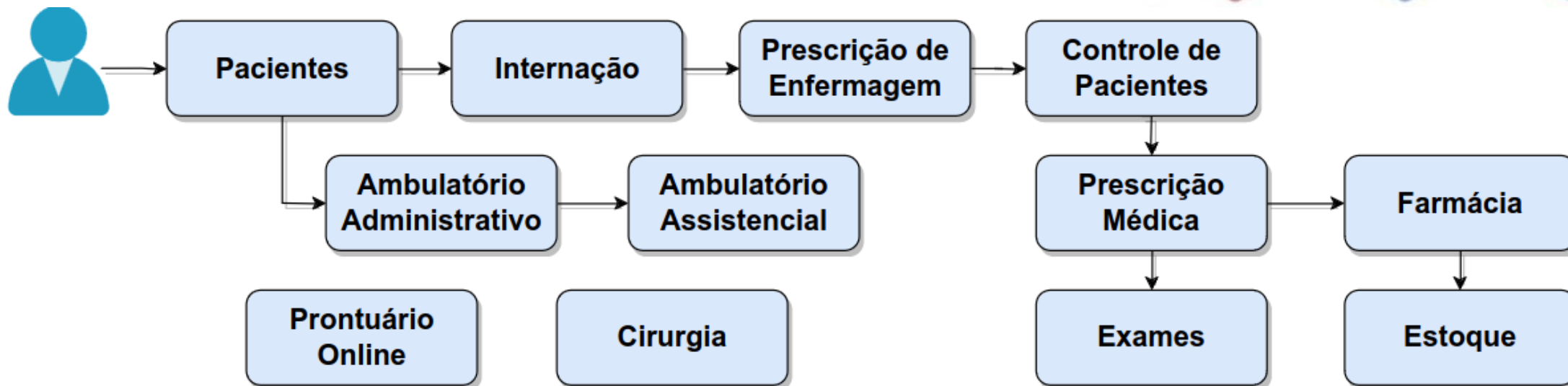
- **AGHUX** → Aplicativo de Gestão para Hospitais Universitários
 - Desenvolvido pela **Empresa Brasileira de Serviços Hospitalares (EBSERH)**
 - Implantado em **41** hospitais da Rede EBSEH
- **Principais Objetivos**
 - Gestão e padronização das práticas assistenciais e administrativas
 - Acesso integrado a todos os EMR gerados pelos hospitais integrantes da rede
- **Benefícios Diretos**
 - Visão transversal sobre a trajetória clínica do paciente
 - Continuidade de tratamentos e atendimentos
 - *Independente do hospital universitário de origem*



AGHUX

Arquitetura

- **Composição** → atualmente contém 12 módulos independentes implementados
 - Dedicados a funções **administrativas e a procedimentos médicos**



REGIÃO CENTRO OESTE

HC-UFMG													
HUB-UnB													
HUJM-UFMT													
HUMAP-UFMS													
HU-UFGD													

REGIÃO SUDESTE

HC-UFMG													
HC-UFTM													
HC-UFU													
HUAP-UFF													
HUCAM-UFES													
HUGG-Unirio													
HU-UFJF													
HU-UFSCar													

REGIÃO NORTE

CHU-UFPA (HUBFS)													
CHU-UFPA (HUJBB)													
HDT-UFT													
HUGV-UFAM													
HU-UNIFAP													

REGIÃO SUL

CHC-UFPR (HC)													
CHC-UFPR (MVFA)													
HE-UFPeI													
HU-FURG													
HUSM-UFMS													
HU-UFSC													

AGHUX

HU Digital

- **O que é?**
 - Plataforma digital para **acesso remoto** às informações médicas registradas no AGHUX
- **Onde está disponível?**
 - Portal *web*
 - Aplicativos em dispositivos móveis
- **Interfaces de usuário distintas**
 - Profissional de Saúde
 - *Consulta a sumários de alta, procedimentos e cirurgias realizadas ou agendadas*
 - Paciente
 - Acesso aos próprios históricos de dados
 - *Outros serviços digitais...*



HU Digital

Para acessar o aplicativo realize o login com gov.br

[Entrar com gov.br](#)

[FAQ](#) [Termo de uso e aviso de privacidade](#)

[Fale com a EBSEERH](#)

[gov.br](#) [EBSEERH](#)
HOSPITAL UNIVERSITÁRIO FEDERAL

16:34 95%
Voz LTE+
HU Digital

[Início](#)

Olá, Nicollas Rodrigues De Oliveira!

[Atestados e prescrições](#)
Acesse seus atestados, solicitações de exames e procedimentos

[Teleatendimento](#)
Acesse suas teleconsultas

[Meus registros](#)
Acesse seus registros clínicos e resultados de exames

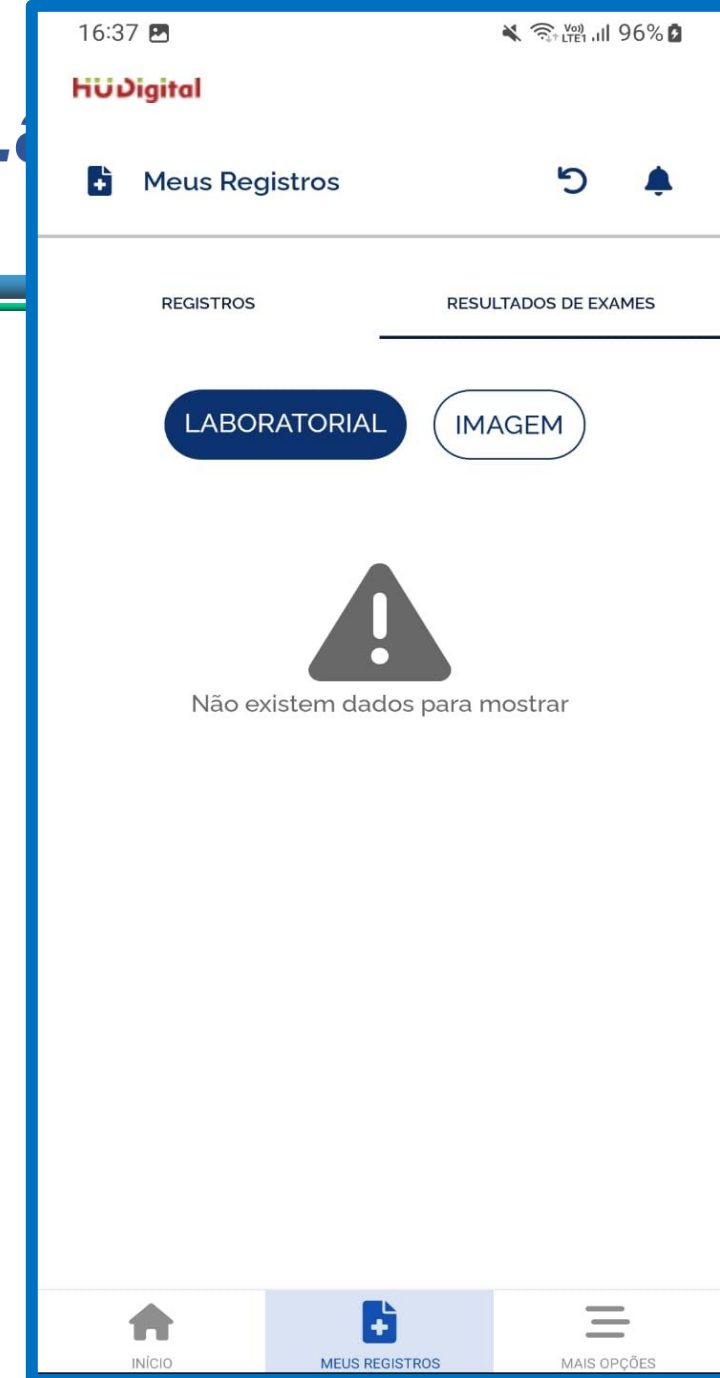
[Compartilhamentos](#)
Gerencie o compartilhamento dos seus registros e consentimentos

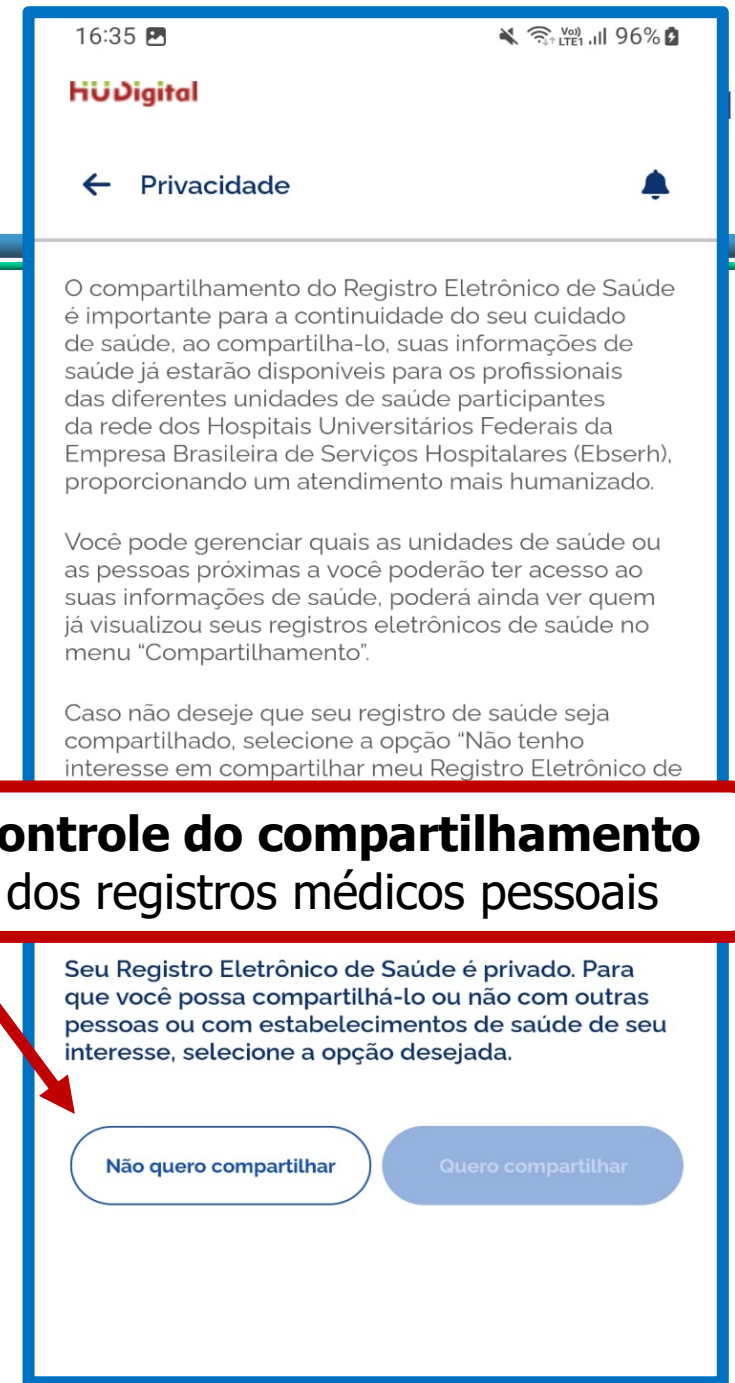
[INÍCIO](#) [MEUS REGISTROS](#) [MAIS OPÇÕES](#)

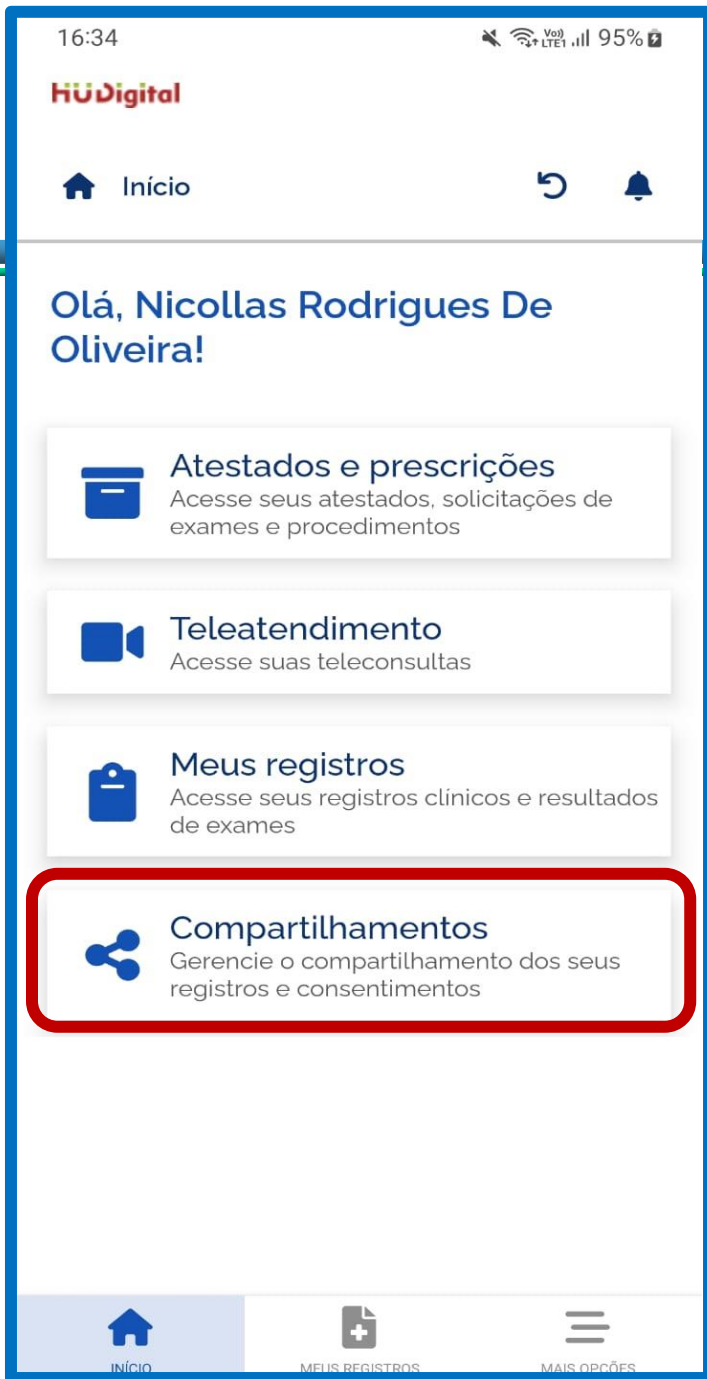
AGHUX

HU Digital

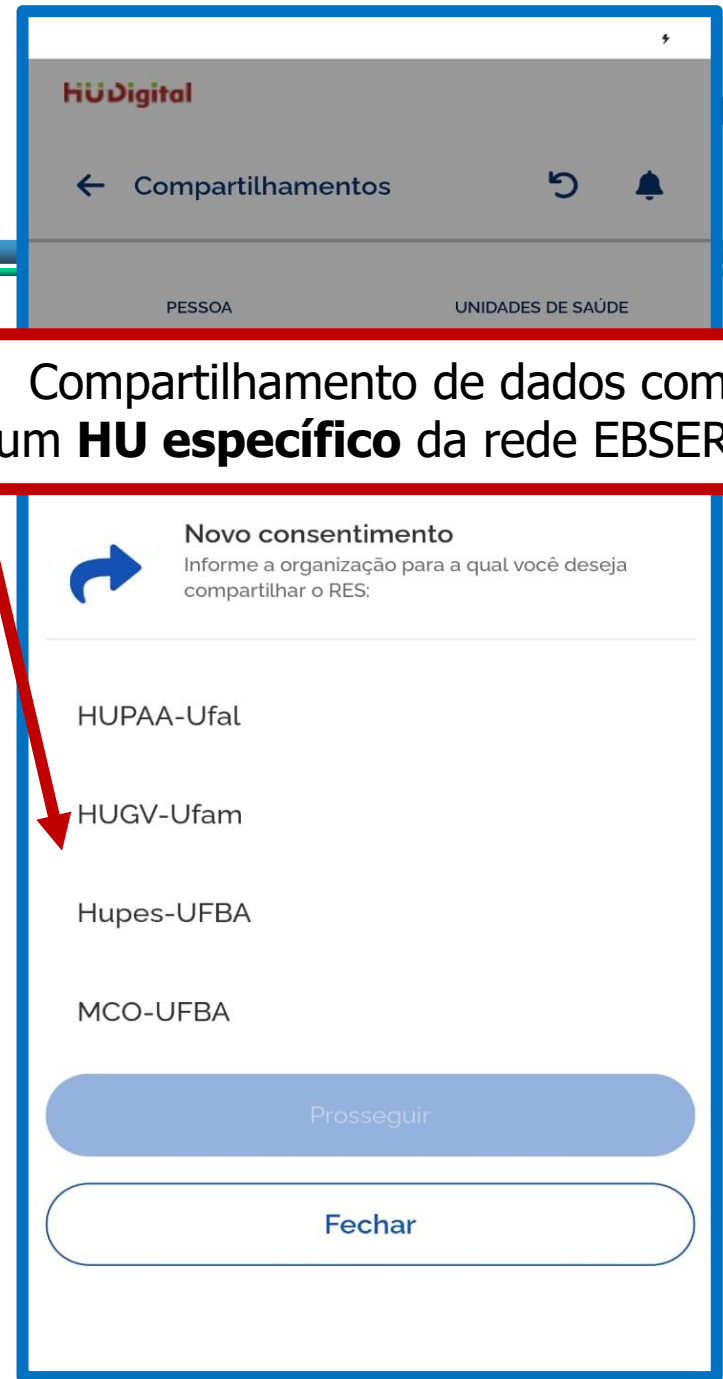
- **Interfaces de Usuário - Paciente**
 - Acesso ao próprio histórico EMR
 - *Exames Laboratoriais*
 - *Exames de Imagem*
 - outros serviços digitais...
 - Emissão de certificados
 - Realização de teleconsultas
 - Controle da permissão de acesso
 - *Podendo ser concedida a..*
 - Pessoas físicas; ou
 - Hospitais Universitários específicos da rede







Compartilhamento de dados com outra **pessoa física cadastrada**



Compartilhamento de dados com um **HU específico** da rede EBSEH



- **Desafios Encontrados na Implementação**

- Resistência à mudança
- Equipes de TI reduzidas ou inexistentes
- Processos indefinidos
- Envolvimento de governança
- Modificações infraestruturais



- **Principal Dificuldade** → Atualmente

- Descompasso de desenvolvimento dos módulos
- Módulos implementados podem estar em versões distintas
 - **Consequência**
 - Prejuízo à integração dos dados dentro da Rede EBSE RH

Abordagens Tradicionais

GestãoDS

- **GestãoDS** → *software* médico comercial hospedado em nuvem
 - Dedicado a auxiliar a **gestão de clínicas e consultórios**
 - Oferece conformidade à LGPD e à HIPAA
 - **Funcionalidades** (inclusas ou não dependendo do plano)
 - Agendamento *online* de consultas e telemedicina
 - Gestão financeiro → controle do faturamento e custos
 - Ações de marketing digital
 - Visualização dos dados → Dashboard interativo
 - Personalização de prontuários e prescrições conforme a especialidade do profissional
 - Dermatologia, Cirurgia Plástica, Oftalmologia, Pediatria e Obstetrícia
 - **Controle de Acesso**
 - **Baseado em perfis de usuário**
 - Fornecendo vários níveis de permissão de acordo com o profissional



- **iDoc** → *software* médico comercial para radiologia odontológica



- **Principais Objetivos**

- Criação, processamento, gestão e distribuição *on-line* de documentações e imagens odontológicas
- Acesso aos dados dos pacientes pelo dentista
 - Mesmo quando o exame é realizado em clínicas radiológicas distintas

- **Funcionalidades**



- **Cadastro de pacientes** para criação de documentações odontológicas



- **Processamento inteligente das imagens**
 - Permitindo a classificação, recorte, alinhamento, descrição e medições



- **Integrações com sistemas terceirizados**
 - Tanto sistemas de convênio quanto de gestão financeira



- **Segurança** na gestão, armazenamento e encaminhamento de imagens
 - Para radiologistas, laudadores e pacientes



- **Visualizadores interativos** de imagens, volumes 3D e diversos exames
 - Compatível com diferentes formatos: JPEG, DICOM, STL, PLY, PPTZ, DOCX e PDF



- **Site Responsivo**
 - Versão exclusiva para pacientes



- **Infraestrutura em nuvem**
 - Hospedagem na AWS
 - Dispensa instalação e configuração de programas locais



FLUXO TRADICIONAL



FLUXO DIGITAL



- **Alert** → *software* comercial de **gerenciamento do processo clínico eletrônico**
 - Engloba diversos aplicativos
 - Adaptado para **web e nuvem**
- **Benefícios**
 - Reduzir erros médicos
 - Melhorar os resultados clínicos
 - Aumentar a satisfação do paciente e segurança na área da saúde
 - Melhorar a experiência de trabalho de profissionais de saúde
- **Principais Funcionalidades**
 - Histórico dos pacientes e gestão de pedidos
 - Agendamento, teleatendimento e alertas de consultas ou procedimentos médicos
 - Atribuição de altas e emissão de relatórios
 - Sistema interno de planejamento e de inteligência empresarial



Alert

Características

- **Compatibilidade**
 - **Padrões de interoperabilidade e suporte**
 - IHE, HL7 e ITIL
 - **Terminologias internacionais**
 - SNOMED, ICD, LOINC
- **Single Sign-On (SSO)**
 - Mecanismo de **autenticação unificada** independente da aplicação Alert
- **Controle de acesso**
 - **Baseado em perfis de usuário**
 - Associados a cada profissional cadastrado no sistema

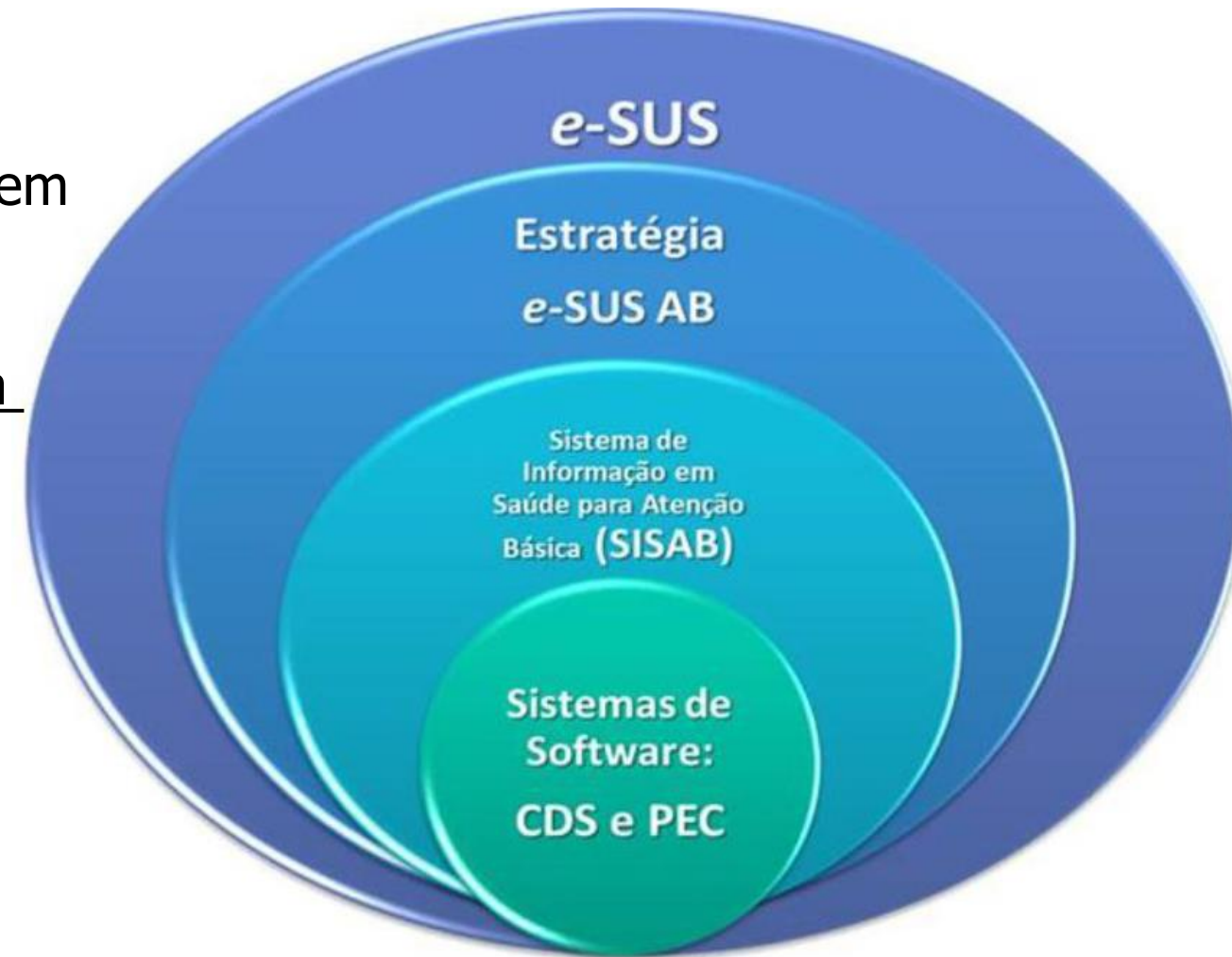
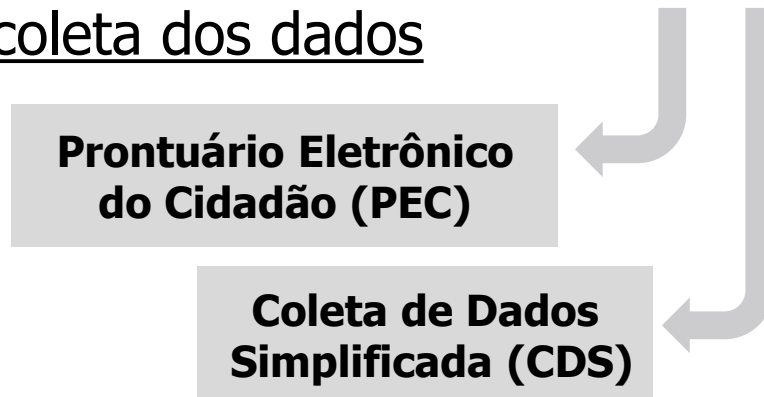


- **e-SUS Atenção Primária (APS)** → sistema eletrônico governamental
 - Reúne ferramentas voltadas para a **reformulação da Atenção Básica (AB)**
 - Desenvolvido e mantido pelo **Ministério da Saúde (MS)**
- **Objetivos**
 - Informatizar as unidades do **Sistema Único de Saúde (SUS)**
 - Individualizar o registro das informações em saúde
 - Integrar os diversos sistemas de informação oficiais existentes na AB
 - Reduzir o retrabalho na coleta de dados
- **Controle de Acesso**
 - **Baseado em perfis de acesso** ou papéis
 - Cada perfil é associado a um conjunto de recursos do sistema **ativos** ou **inativos**
 - Dependendo das atividades desenvolvidas pelo profissional



e-SUS Atenção Primária (APS) Composição

- **e-SUS Atenção Primária (APS)**
 - **Principais Componentes**
 - **SISAB** → Sistema de Informação em Saúde para a Atenção Básica
 - **Sistema e-SUS AB**
 - Composto por 2 softwares para coleta dos dados
 - **Apps para Sistemas Móveis**
 - e-SUS Território



- **SISAB → Sistema de Informação em Saúde para a Atenção Básica**

- **Principais Funções**

- **Centralização** nacional do processamento
 - Independentemente dos *software* de coleta, seja ele...
 - Prontuário Eletrônico do Cidadão (PEC)
 - Coleta de Dados Simplificada (CDS)
 - Sistema terceirizados
- **Disseminação de dados** e informações relacionadas à AB
- Emissão de **relatórios de desempenho**
 - Contendo indicadores de saúde por...
 - Estado, Município, Região de Saúde, Equipe



- **Apps de Sistemas Móveis**

- Utilizado em *tablets* ou *smartphones*
- Usado *offline* por agentes de saúde em locais de difícil manejo de *notebooks*



- **e-SUS Território**

- **Funções**

- Registrar as características sociosaniatárias e sociodemográficas dos domicílios
- Registrar problemas e condições de saúde do ambiente residido pelo paciente



- **e-SUS Atividade Coletiva**

- **Função**

- Registrar digitalmente os dados das atividades coletivas



- **e-SUS Vacinação**

- **Função**

- Registrar vacinas aplicadas¹⁸⁴ pela equipe fora da unidade básica de saúde

e-SUS Atenção Primária (APS)

Composição

- **Prontuário Eletrônico do Cidadão (PEC)** → 1º *software* de coleta de dados do e-SUS
 - Instalável no **Windows e Linux** → atualmente na versão 5.1.20
 - **Função Principal**
 - Armazenar todas as informações clínicas e administrativas do paciente
 - **Funcionalidades**



e-SUS Atenção Primária (APS)

Coleta de Dados Simplificada (CDS)

- **Coleta de Dados Simplificada (CDS)** → 2º *software* de coleta de dados do e-SUS
 - Também instalável no Windows e Linux
- **Principal Função**
 - **Estruturar a digitação** do cadastro e das fichas de atendimento
- **Funcionamento *Off-line***
 - Permite a inserção de dados de forma *off-line*
 - Posterior **consolidação através de um PEC com acesso à Internet**
- **Benefícios**
 - Menos fichas de atendimento em papel
 - Individualização dos dados dos cidadãos
 - Relatórios de saúde dinâmicos



e-SUS Atenção Primária (APS)

Coleta de Dados Simplificada (CDS)

- **Coleta de Dados Simplificada (CDS)** → 2º *software* de coleta de dados do e-SUS
 - **Limitações**
 - Baixa capacidade de armazenamento local → **banco de dados embarcado**
 - Ausência de funções gerenciais
 - **Módulos**

Cadastro individual



Cadastro domiciliar



Ficha de atendimento individual



Ficha de atendimento odontológico



Ficha de atividade coletiva



Ficha de procedimentos



Ficha de visita domiciliar



Coleta de Dados Simplificada (CDS)

Módulo de Cadastro

Inclusão dos dados relacionados ao...

- **Cadastro Nacional de Estabelecimento de Saúde (CNES)**
 - Vinculando a UBS e os profissionais responsáveis
- **Cadastro do Indivíduo**
 - Ex: Dados Pessoais, Cartão Nacional de Saúde



PEC > CDS > Cadastros individuais > Adicionar

Compatível com a FCI / e-SUS AB v.2.1.0

CNS do profissional * CBO CNES INE Data *

Identificação do usuário / cidadão

CNS do cidadão Cidadão é o responsável familiar? Sim Não CNS do responsável familiar

Nome completo * Microárea * Fora da área

Nome social Data de nascimento * Sexo * Feminino Masculino

Raça / Cor * Branca Preta Parda Amarela Indígena Etnia Nº NIS (PIS / PASEP)

Nome completo da mãe * Desconhecido

Nome completo do pai * Desconhecido

Nacionalidade * Brasileira Naturalizado Estrangeiro País de nascimento Data de naturalização Portaria de naturalização

Município e UF de nascimento Data de entrada no Brasil Telefone celular E-mail

- **Adaptabilidade às UBSs com diferentes condições estruturais**
 - **Cenários com Infraestrutura**
 - Com informatização e conectividade de qualidade e estável
 - **Cenários sem Infraestrutura**
 - Sem informatização
 - Com conectividade limitada ou instável
 - Com conectividade inexistente
- **Integração com sistemas terceirizados/próprios**
 - Viabilizada através da API do **Apache Thrift** ou adotando arquivos no formato **XML**
 - **Principal Benefício**
 - Garantia de interoperabilidade do e-SUS APS com sistemas existentes
 - Permite a importação dos dados coletados e a consolidação no SISAB



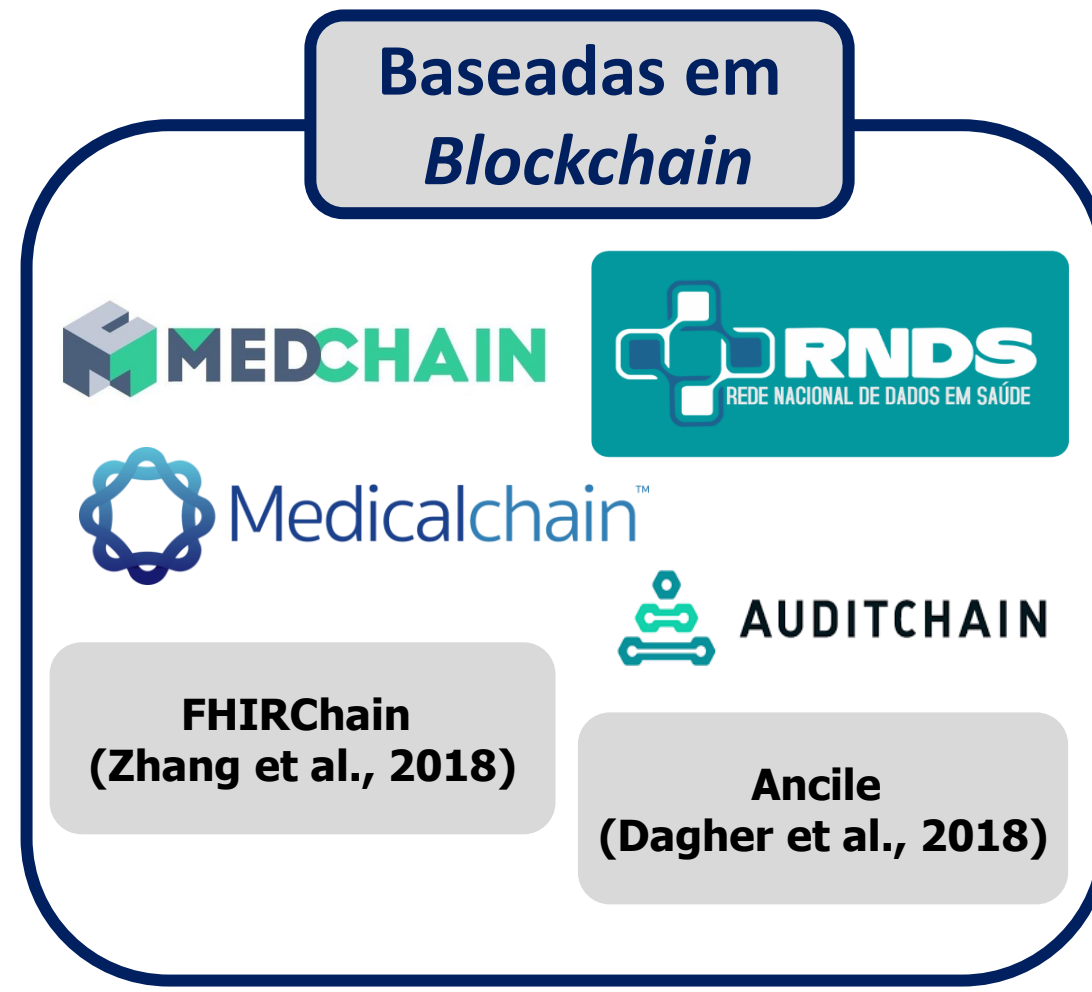
e-SUS Atenção Primária (APS)

Integração com Sistemas Terceirizados



Soluções de Integração e Compartilhamento

Abordagens Baseadas em *Blockchain*



Abordagens baseadas em *Blockchain*

MedChain



- **MedChain** → solução comercial
 - Plataforma adotadas
 - **Hyperledger Fabric e Ethereum**
- **Características**
 - **Uso de dois tipos de *tokens***
 - *tokens* externos (MedCoins) → fornece controle de acesso e privacidade
 - *tokens* internos (Record Tokens) → fornece um mapa do registro do paciente distribuído
 - Adicionando resumos criptográficos à cadeia de blocos
 - **Suporte a diferentes formatos de registro**
 - Texto simples, imagens digitais ou objetos de banco de dados
 - **Armazenamento em sistema de arquivos distribuído**
 - Endereço do registro de um paciente armazenado é associado ao **bloco de paciente** daquele paciente na Ethereum



Abordagens baseadas em *Blockchain*

AuditChain

- **AuditChain** → solução acadêmica
 - Utiliza a plataforma **Hyperledger Fabric**
 - Emprega **contratos inteligentes**
- **Caraterísticas**
 - **Controle de Acesso** → Multinível
 - Pacientes, médicos, enfermeiros e administradores hospitalares atuam no gerenciamento de EMRs
 - **Assinatura Digital da Transação**
 - Criptografia de chave pública e serve como um *token* virtual para controle de acesso



AUDITCHAIN

- **Ancile** → solução acadêmica para gerenciamento de registros de saúde
 - Utiliza a plataforma **Hyperledger Fabric**
 - Emprega **contratos inteligentes**
 - Para maior controle de acesso e ofuscação de dados
- **Características**
 - Prevê a manutenção dos registros médicos dos pacientes → **em bancos de dados existentes dos provedores**
 - Endereços de referência a esses registros + suas permissões → armazenados no contrato inteligente
 - 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

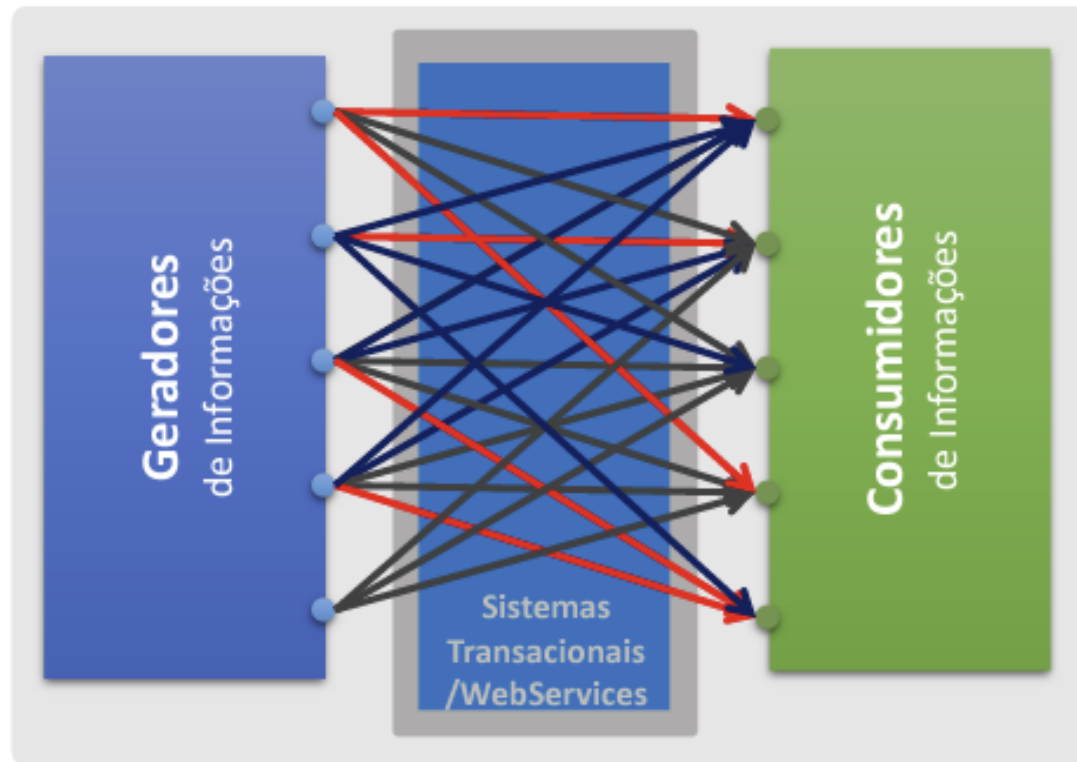
- **Rede Nacional de Dados em Saúde - (RNDS)** → solução governamental
 - Plataforma nacional de **interoperabilidade e troca de dados** em saúde
 - Inicialmente desenvolvida em 2020 → **Previsão de conclusão em 2028**
- **Principais Objetivos**
 - Promover a criação de um Prontuário Único de Saúde
 - Através da troca de informações entre os diversos níveis de atenção à Saúde
 - Permitir a transição e continuidade do cuidado nos setores público e privado
- **Benefícios**
 - Aprimoramento no **combate a epidemias** e doenças
 - Maior **transparência** na gestão dos dados
 - Melhoria no **atendimento à população**
 - Maior **eficiência na gestão** dos recursos públicos
 - Acompanhamento da **trajetória do paciente**



Rede Nacional de Dados em Saúde (RNDS)

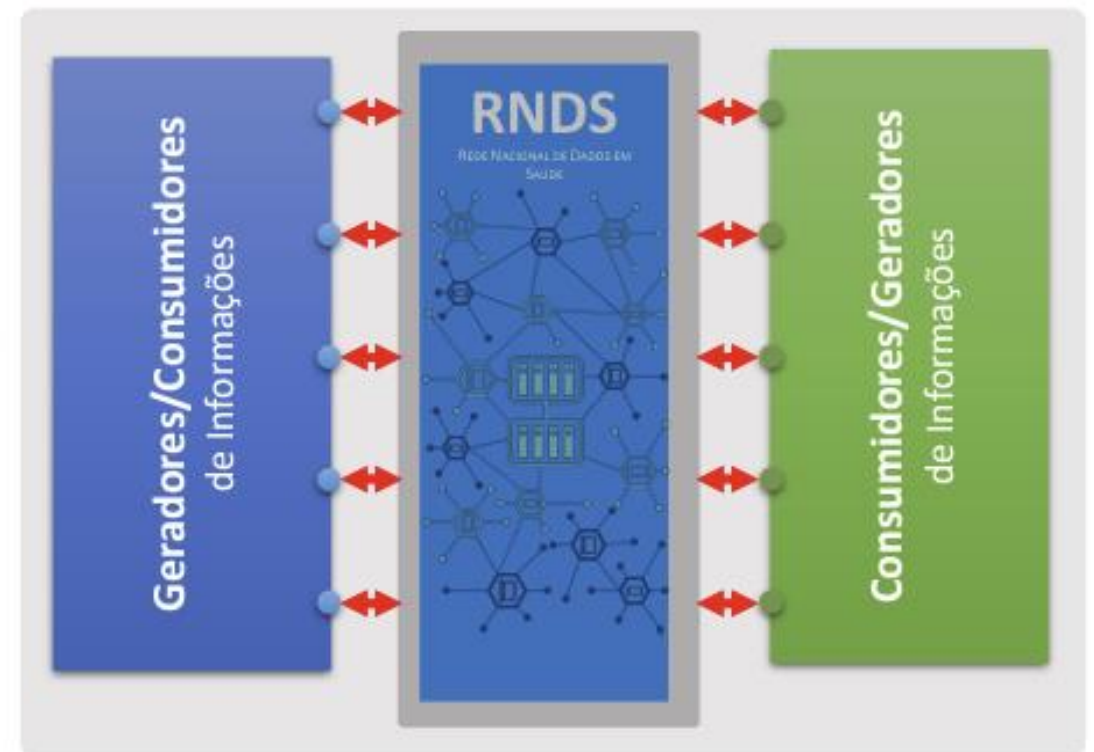
Alteração na Troca de Dados

Troca de Informação de Saúde
Modelo Atual



Fluxo da Informação

Troca de Informação de Saúde
Com a RNDS



Fluxo da Informação

Rede Nacional de Dados em Saúde (RNDS)

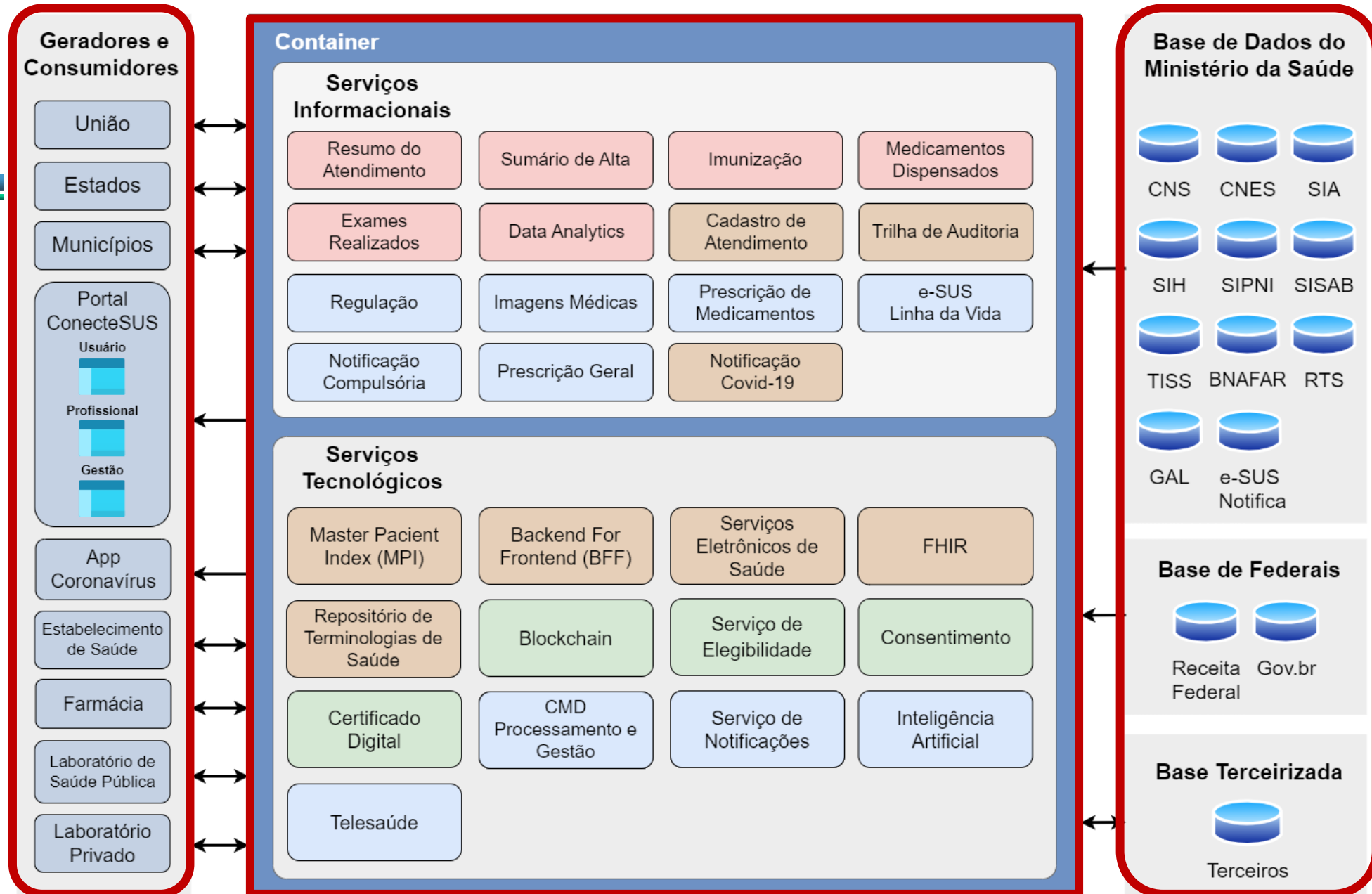
Componentes



- **Infraestrutura Containerizada** (Em desenvolvimento)
 - Hospedagem em Nuvem
 - Contendo **contêineres dedicados e distribuídos** entre os estados federados
 - Cada contêiner é subdividido em...
 - **Serviços Informacionais e Serviços Tecnológicos**
 - Classificados de acordo com...
 - Tipo: **Conjunto Mínimo de Dados** **Serviços de Segurança**
 - Grau de Maturidade: **Serviços Planejados** **Serviços Disponíveis**
- **Geradores e Consumidores de Dados**
 - Entes da Federação, ConecteSUS, App Corona Virus, Estabel. de Saúde e Laboratórios
- **Bases de Dados**
 - Ministério da Saúde, Federais e Terceirizadas

RNDS

Arquitetura



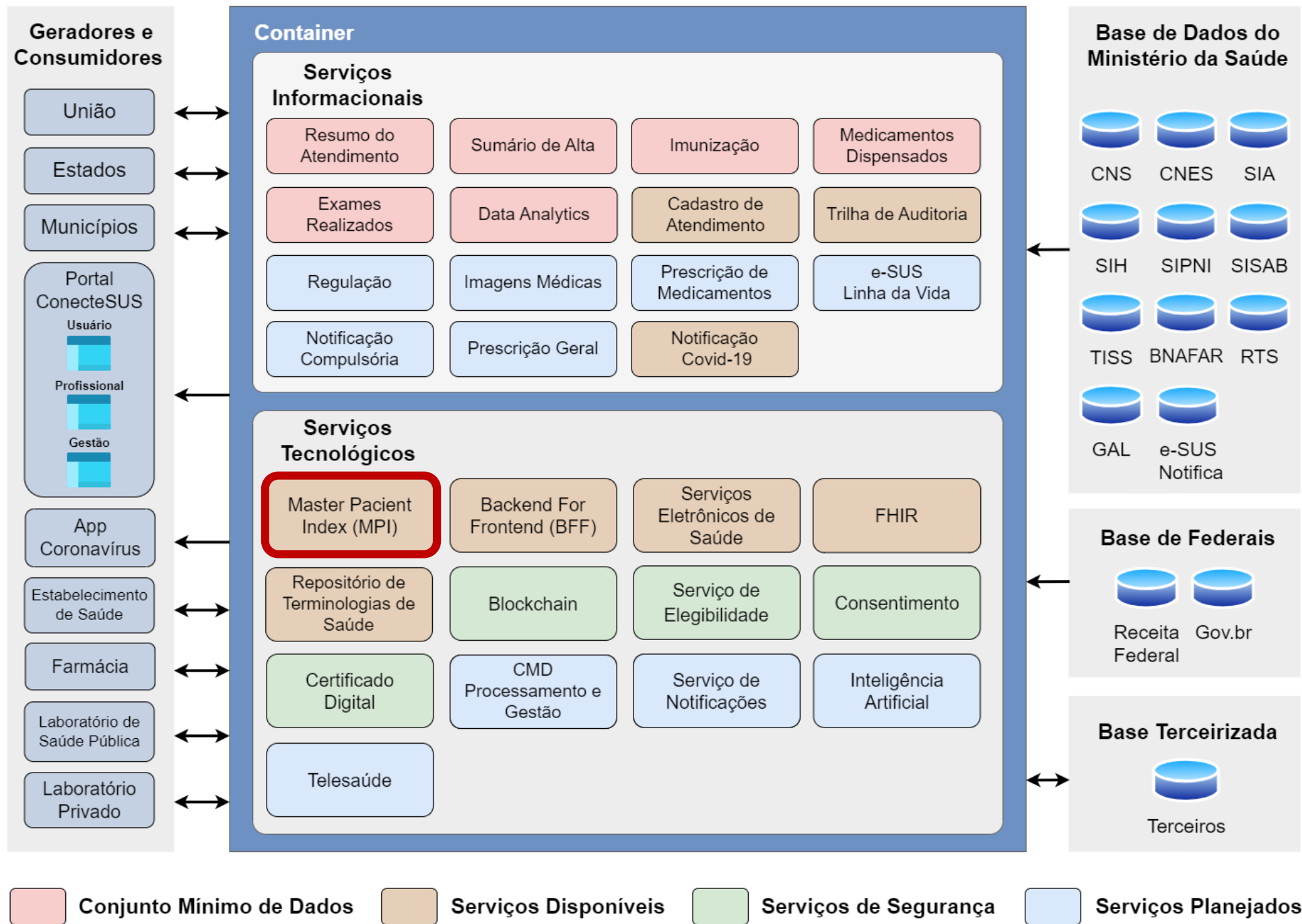
Conjunto Mínimo de Dados Serviços Disponíveis Serviços de Segurança Serviços Planejados

RNDS

Arquitetura

Master Patient Index (MPI)

- Banco de dados que **unifica as informações de cada paciente registrado** por uma organização de saúde

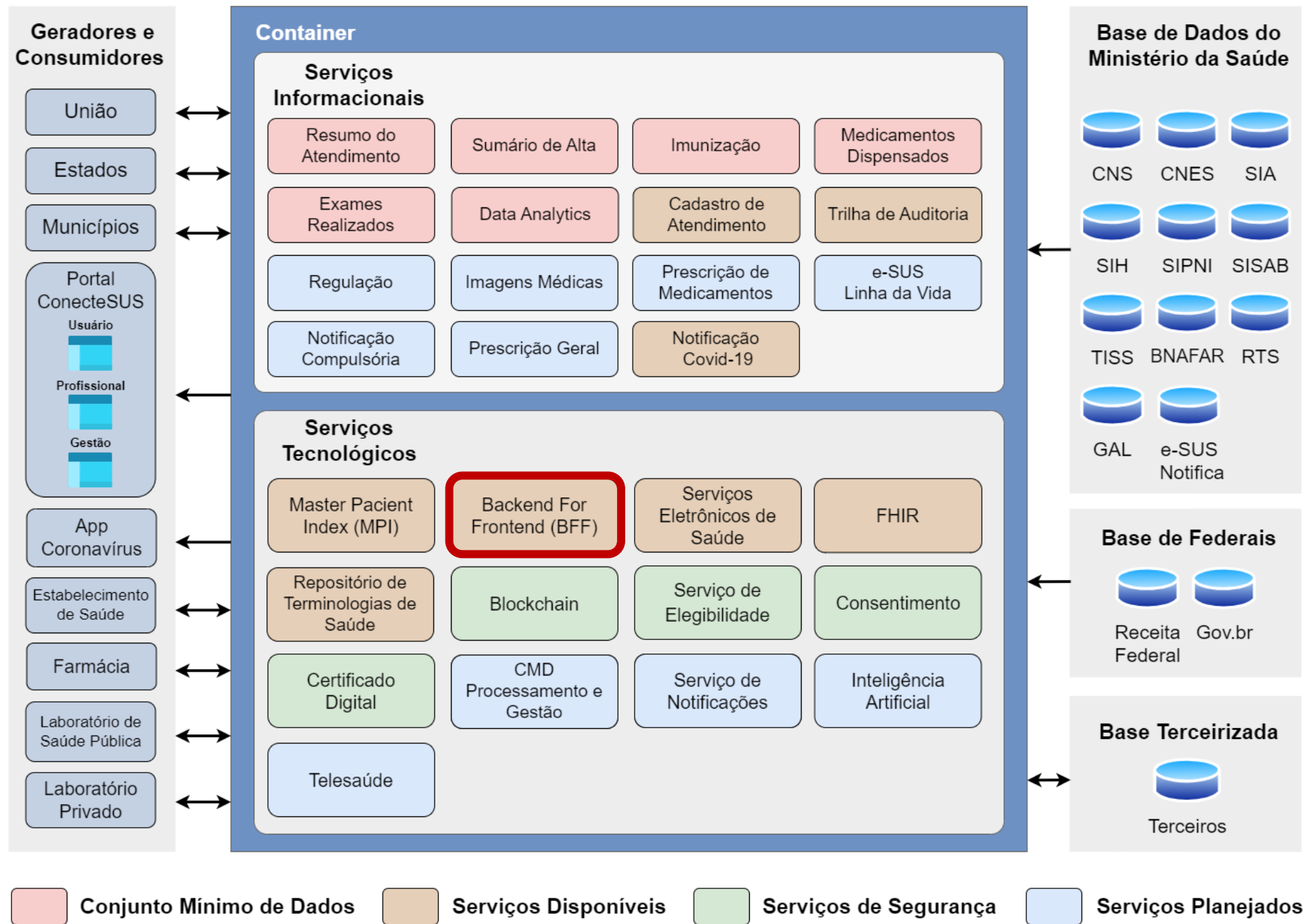


RNDS

Arquitetura

Backend For Frontend (BFF)

- Responsável pela entrega de como as informações serão armazenadas e consultadas
 - Independente da interface gráfica
 - **App ou Portal web**



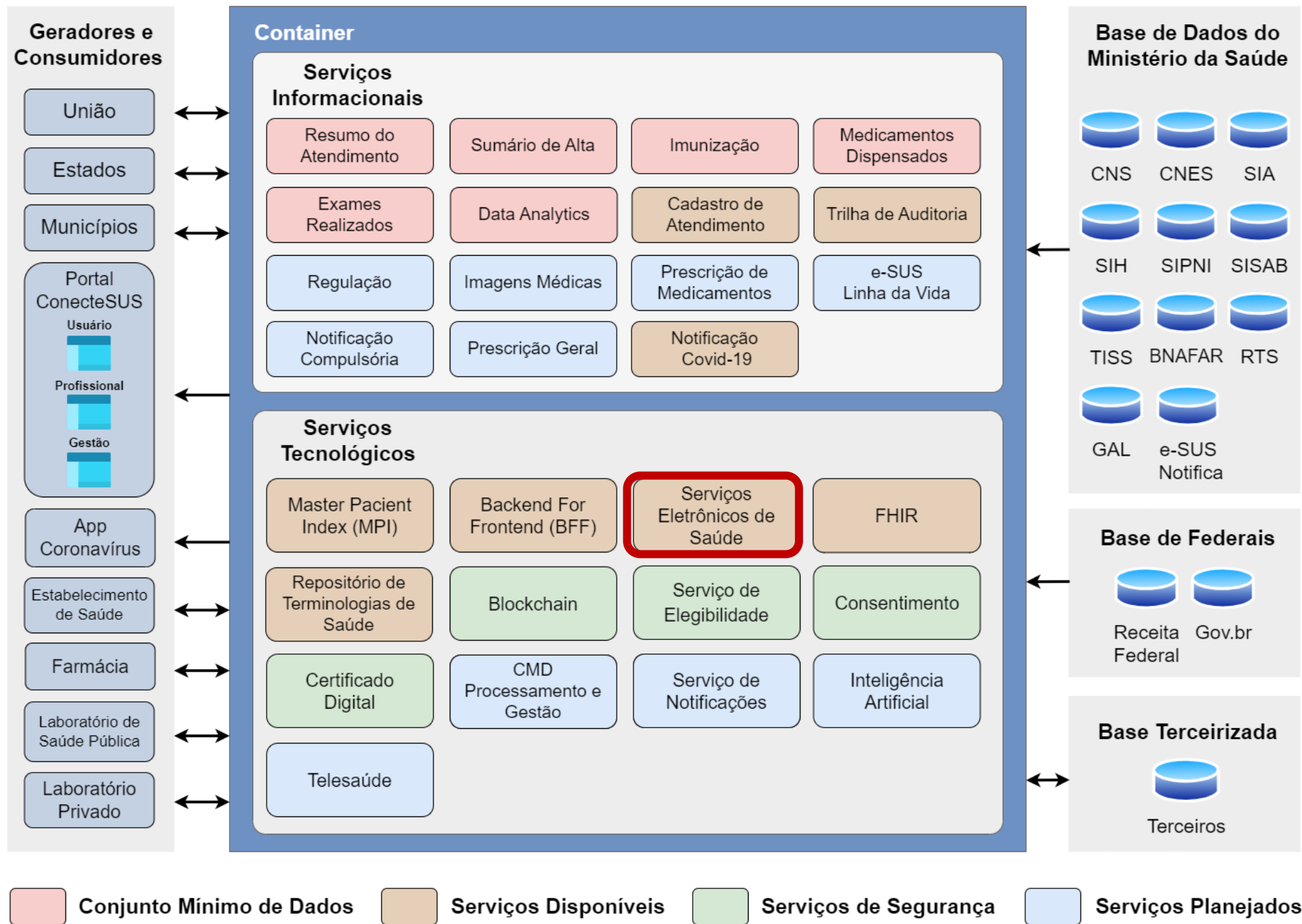
RNDS

Arquitetura

Serviços Eletrônicos de Saúde

- Concentram os serviços RESTful na troca de informações entre as aplicações de Saúde Digital, como

- **PEC**
- **Portais**
- **Aplicações web**

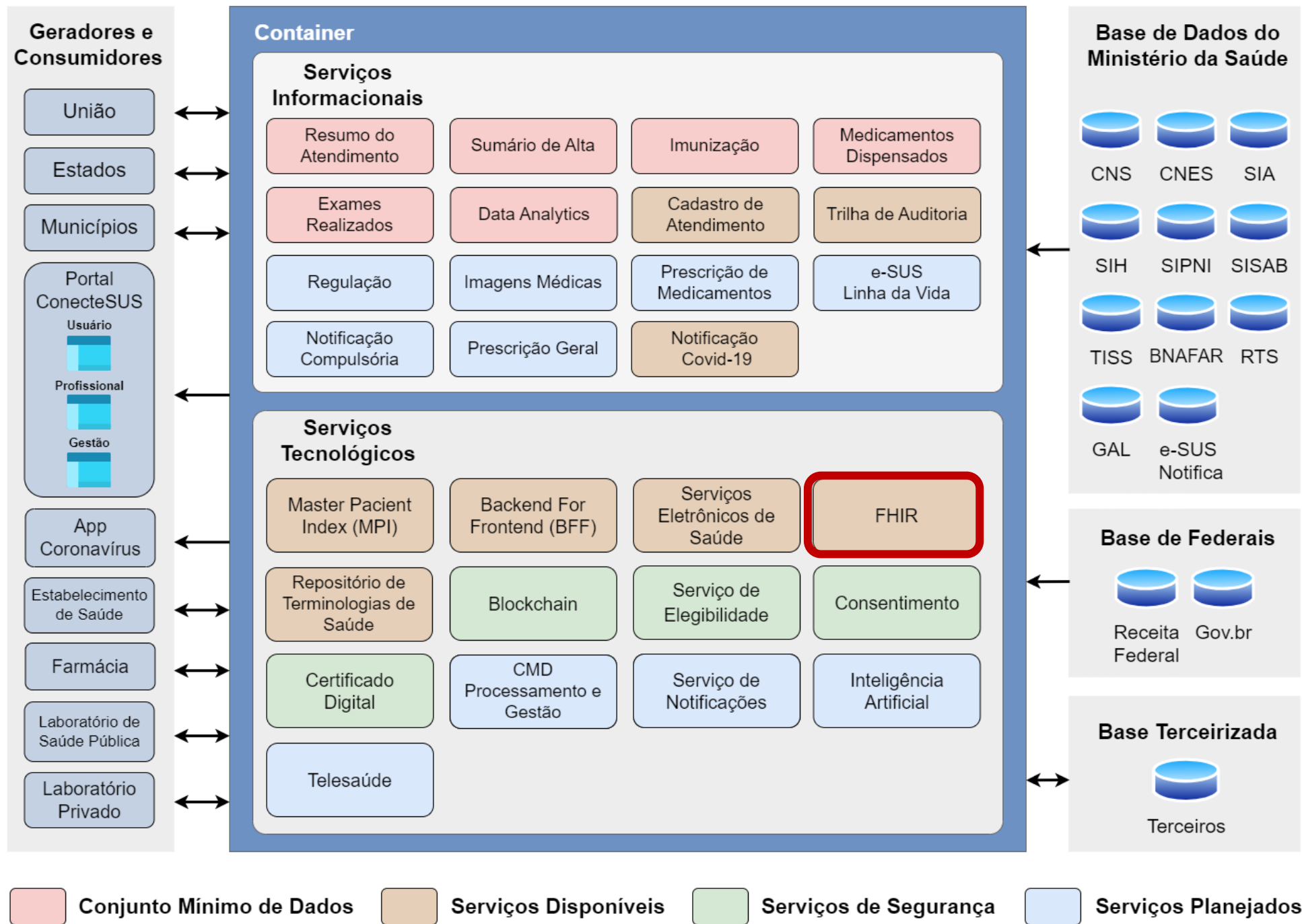


RNDS

Arquitetura

FHIR

- Padrão adotado na troca de informações de saúde entre diferentes estabelecimentos e instituições



RNDS

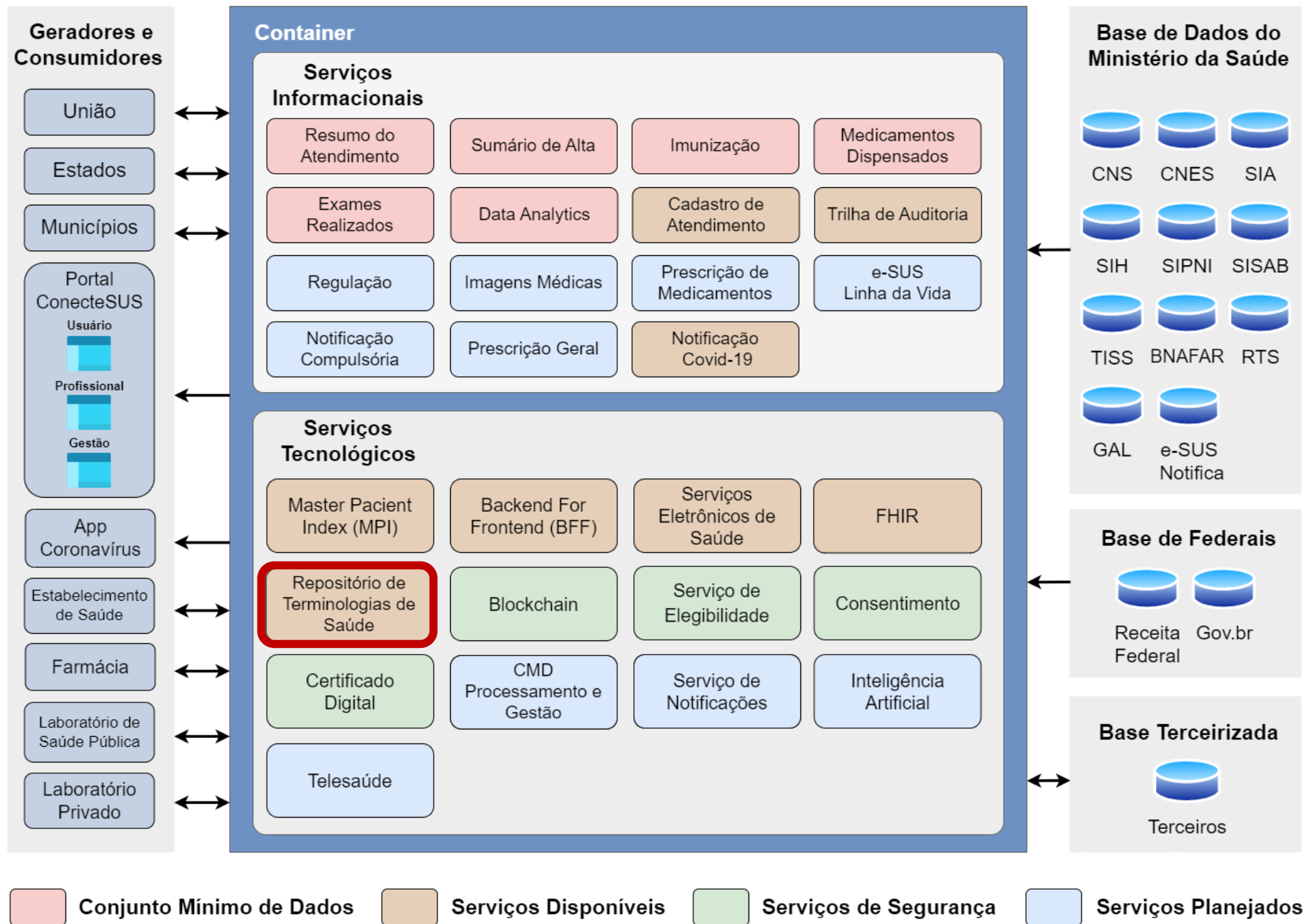
Arquitetura

Repositório de Terminologias de Saúde

- Ambiente virtual nacional que abriga...

classificações,
terminologias,
taxonomias,
modelos de
informação,
nomenclaturas e
definições

...necessárias para
a padronização de
recursos

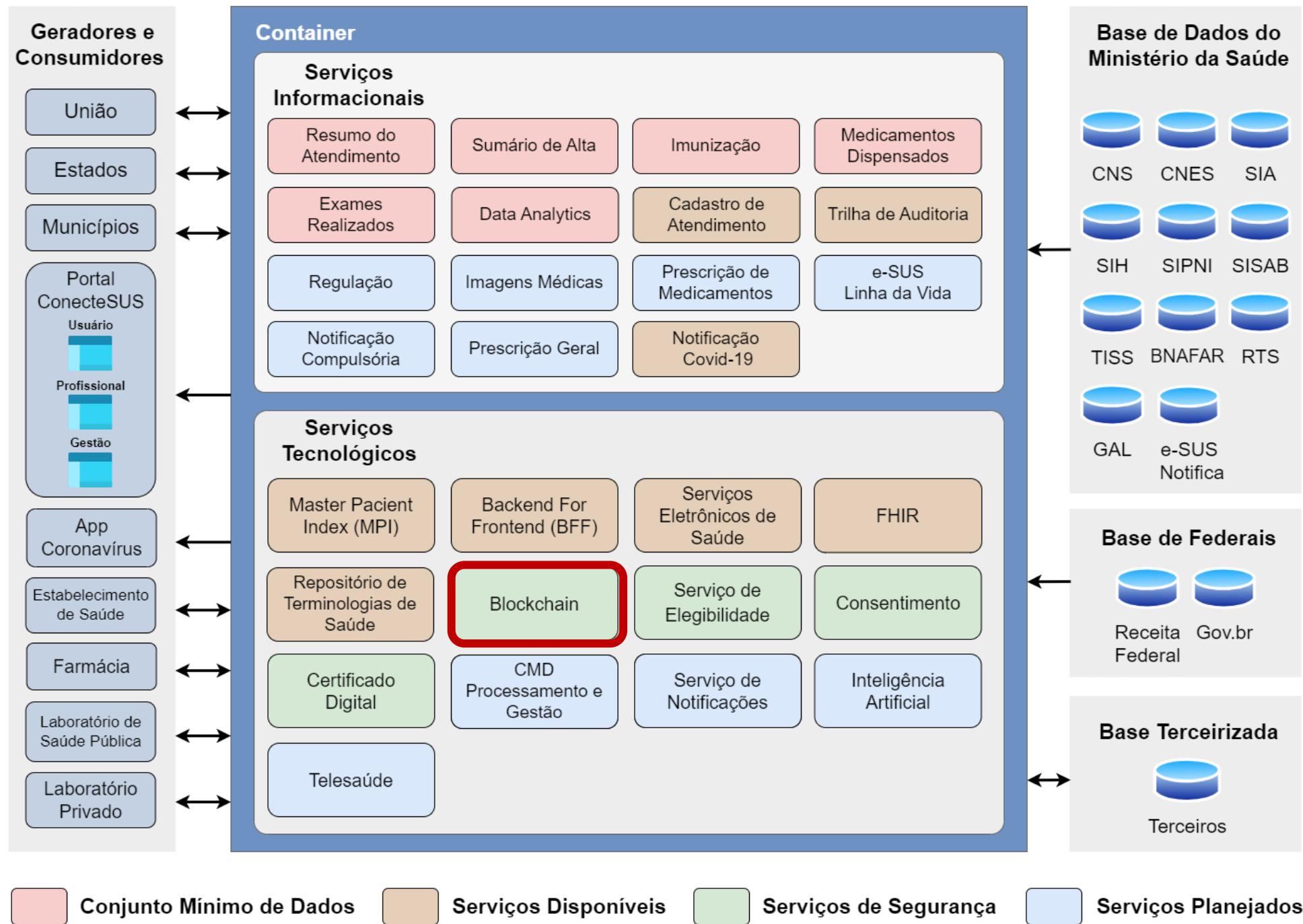


RNDS

Arquitetura

Blockchain

- Cadeia de blocos **privada e permissionada** e baseada na plataforma **Hyperledger Fabric**
- **Raft** → mecanismo de consenso
- **Cada contêiner**
 - Representa um **nó da blockchain**
 - Está localizado em um estabelecimento de saúde



- **Microsserviços de transição**
 - Utilizados para converter dados enviados em **CDA, openEHR e FHIR**
- **Contratos inteligentes**
 - Escritos na linguagem GO
 - **Objetivos**
 - Evitar o preenchimento incompleto ou impressos de registros médicos
 - Assegurar o cumprimento das regras de negócio
 - **Envolvidas nos registros do prontuário eletrônico**
- **Avaliações preliminares** → utilizando Prova de Conceito Arquitetural
 - **Vazão estimada suportada pela RNDS**
 - Até **1.800** transações por segundo (tps) → Taxa Satisfatória
 - Capaz de suportar a quantidade anual de atendimentos prevista no SUS

RNDS

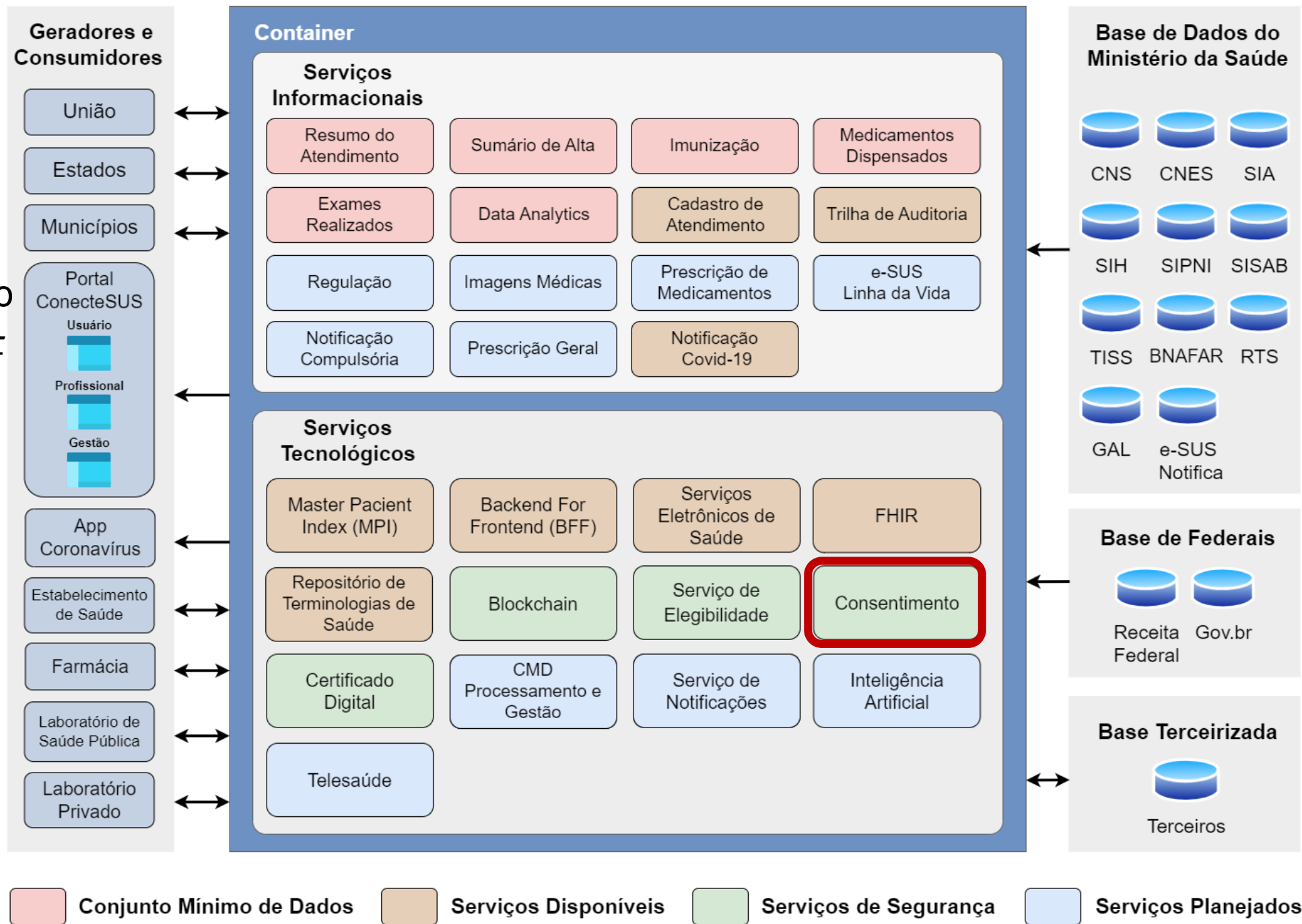
Arquitetura

Consentimento

- Relacionado ao modelo de consentimento *opt-out*

Assume-se um **consentimento Implícito...**

- Até a revogação explícita do consentimento pelo cidadão

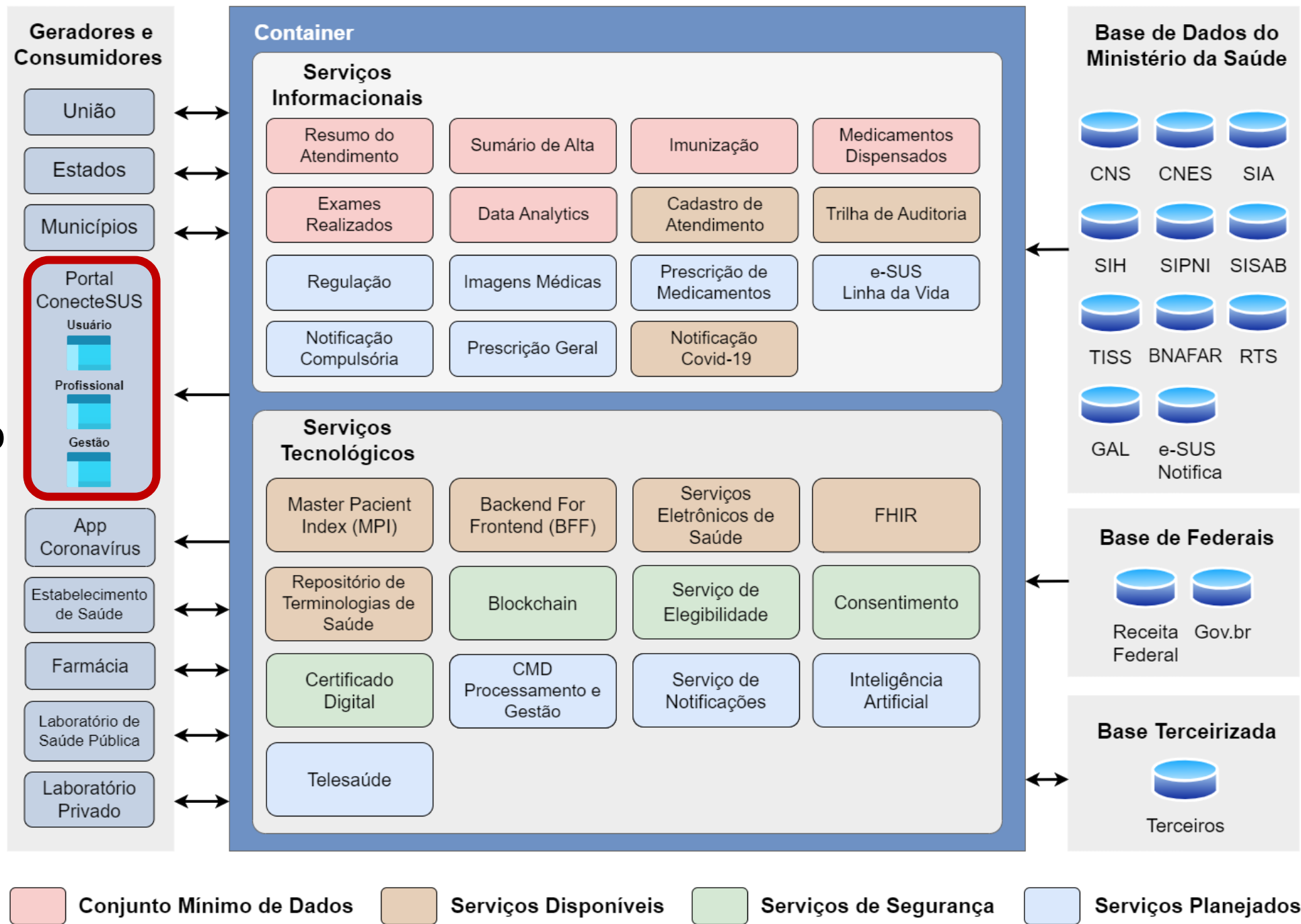


RNDS

Arquitetura

Portal ConecteSUS

- Apresenta 3 versões dependendo do usuário



Rede Nacional de Dados em Saúde (RNDS)

Acesso aos Dados de Saúde



- Histórico Clínico
- Emissão de Certificado de Vacinação
- Resultados de Exames de Covid-19
- Medicamentos (Farmácia Popular)
- Internação e Alergias



- Visualização do Histórico Vacinal e Clínico dos Pacientes
 - Histórico de Atendimentos
- **Promovendo a continuidade do cuidado ao paciente**



- Geração de Relatórios
 - Acompanhar os Indicadores de Saúde
- **Auxiliando a coordenação de políticas públicas**

Rede Nacional de Dados em Saúde (RNDS)

ConecteSUS

Fluxo Operacional

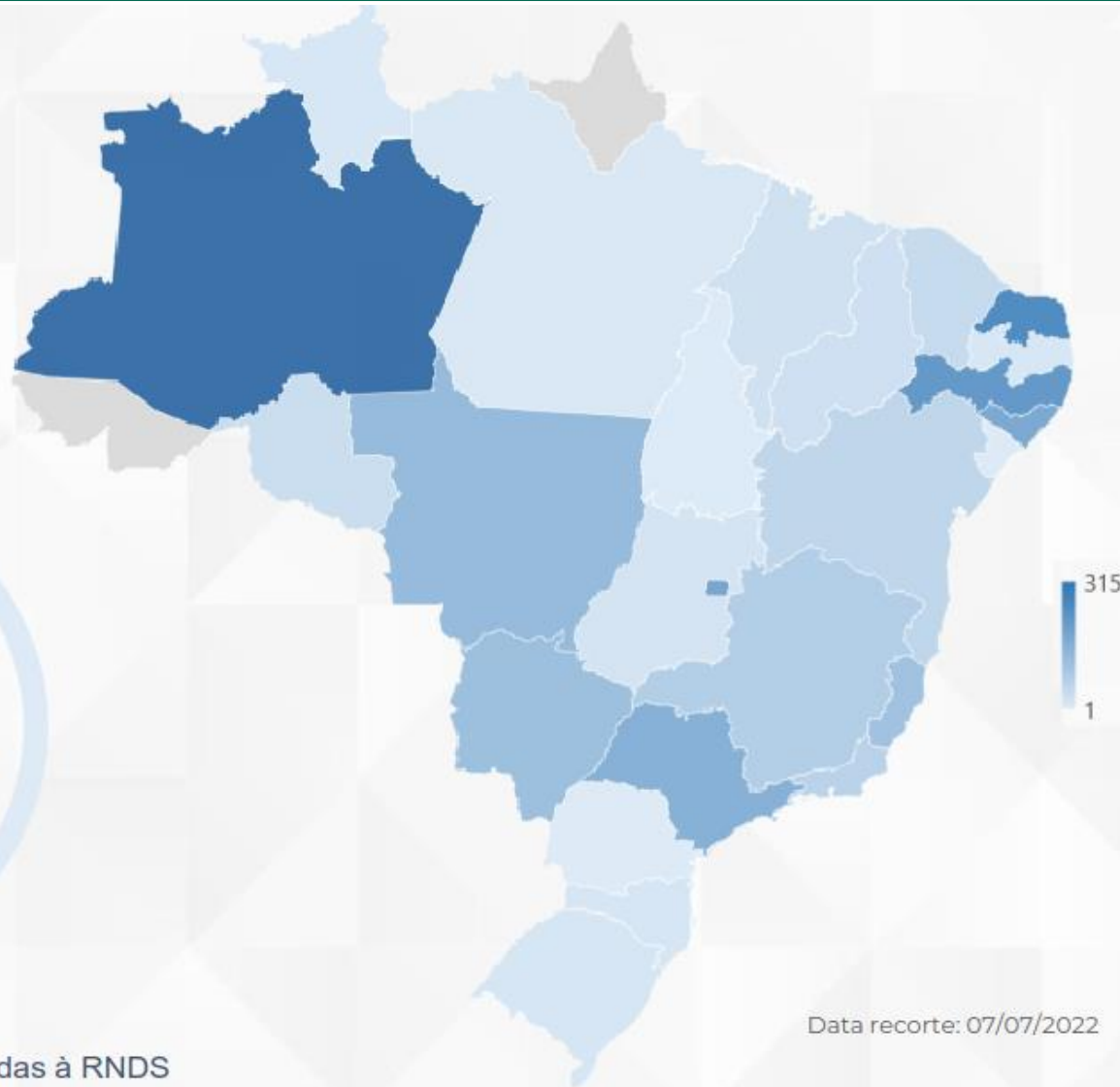


Rede Nacional de Dados em Saúde (RNDS) Estatísticas

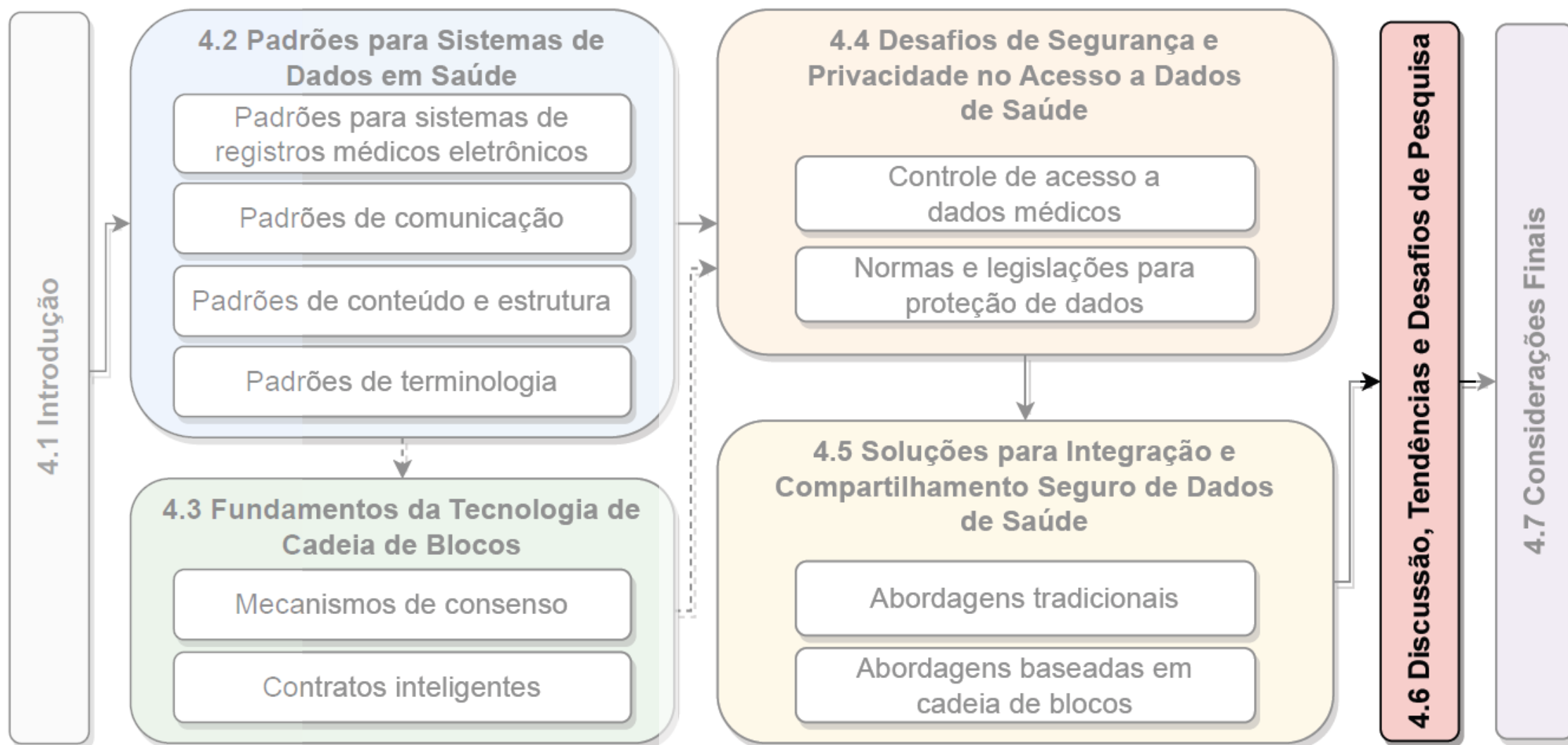


Rede Nacional de Dados em Saúde (RNDS) Estatísticas

Integração das UBS à RNDS



Estados	Qtde. UBS
AC	0
AL	174
AM	315
AP	0
BA	57
CE	43
DF	185
ES	109
GO	19
MA	26
MG	77
MS	116
MT	128
PA	9
PB	11
PE	218
PI	30
PR	1
RJ	64
RN	253
RO	35
RR	12
RS	13
SC	14
SE	1
SP	156
TO	3
Total	2069



Desafios e Oportunidades no Ambiente Médico

Complexidade e Avanços

- Ambiente médico → **complexo** e **constantemente mutável**
- Equipes médicas podem estar **geograficamente distantes**
- **Avanço das Tecnologias na área da saúde**

Adoção de rotinas e procedimentos complexos e atualizações frequentes

Aumenta a demanda de manipulação de dados e a necessidade de segurança e criptografia

Aumenta significativamente a quantidade de dados de saúde digitais disponíveis

Aumento da exigência por medidas de segurança eficazes contra agentes maliciosos

Escalabilidade

- Especialmente desejada em **cadeias de blocos públicas**
 - Limita o número de transações a algumas dezenas por segundo
 - **Latência pelo Processo de Validação** → pode alcançar até 10 minutos
 - Dependendo da plataforma e do mecanismo de consenso

– Causas

- **Escolha inadequada no mecanismo de consenso**
 - Impacta no aumento do tempo de criação de blocos
- Alta dimensionalidade da rede
 - Quanto maior o número de transações e nós...
 - Mais verificações → maior a probabilidade de formação de gargalos

Escalabilidade

- Especialmente impactante em **cadeias de blocos públicas**
 - Limita o número de transações a algumas dezenas por segundo
 - **Latência pelo Processo de Validação** → pode alcançar até 10 minutos
 - Dependendo da plataforma e do mecanismo de consenso

– Causas

– Escolha inadequada no mecanismo de consenso

- Impacta no aumento do tempo de criação de blocos

– Alta dimensionalidade da rede

- Quanto maior o número de transações e nós...
 - Mais verificações → maior a probabilidade de formação de gargalos

Sob a ótica de sistemas de saúde

Atrasos podem afetar adversamente a análise de exames e a definição rápida de diagnósticos

Escalabilidade

- **Abordagens de Mitigação**

- *Sharding*

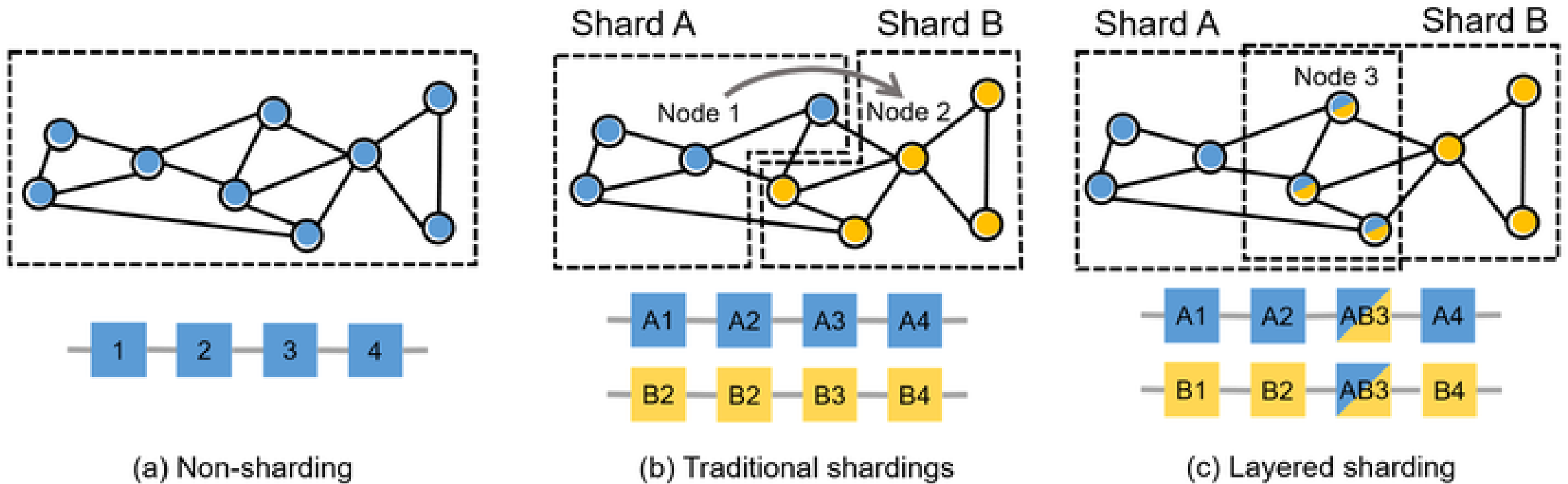
- Técnica baseada na divisão da rede em diferentes fragmentos (*shards*)
 - Evita a tradicional duplicação compulsória da comunicação, do armazenamento de dados e da sobrecarga de computação para cada nó participante

- **Vantagem**

- Desobriga que **cada nó lide com toda carga transacional da rede**
 - Permite que apenas mantenham os dados sobre seu fragmento

Incorporação de *Blockchain* no Setor de Saúde

Principais Obstáculos



Escalabilidade

- **Abordagens de Mitigação:**

- **Grafo Acíclico Direcionado**

(*Directed Acyclic Graph - DAG*)

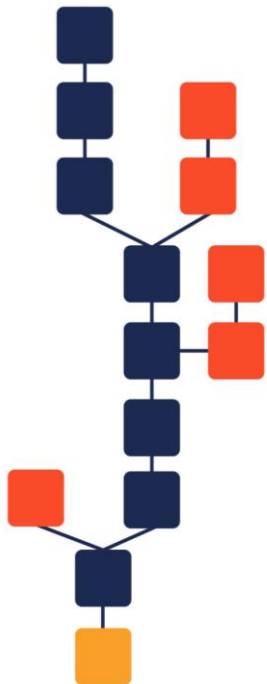
- Modificação da tradicional estrutura linear para uma representação na forma de grafo

- Cada transação é vinculada a múltiplas transações

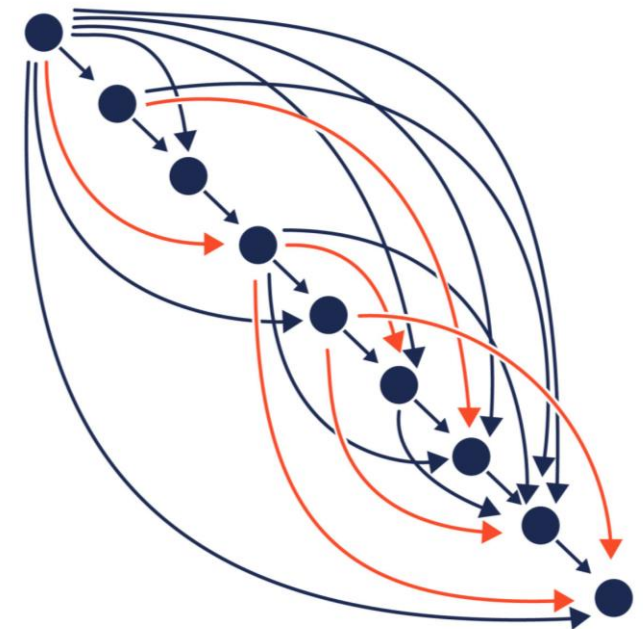
- **Vantagem**

- Paralelismo do processo de validação

Blockchain



DAG

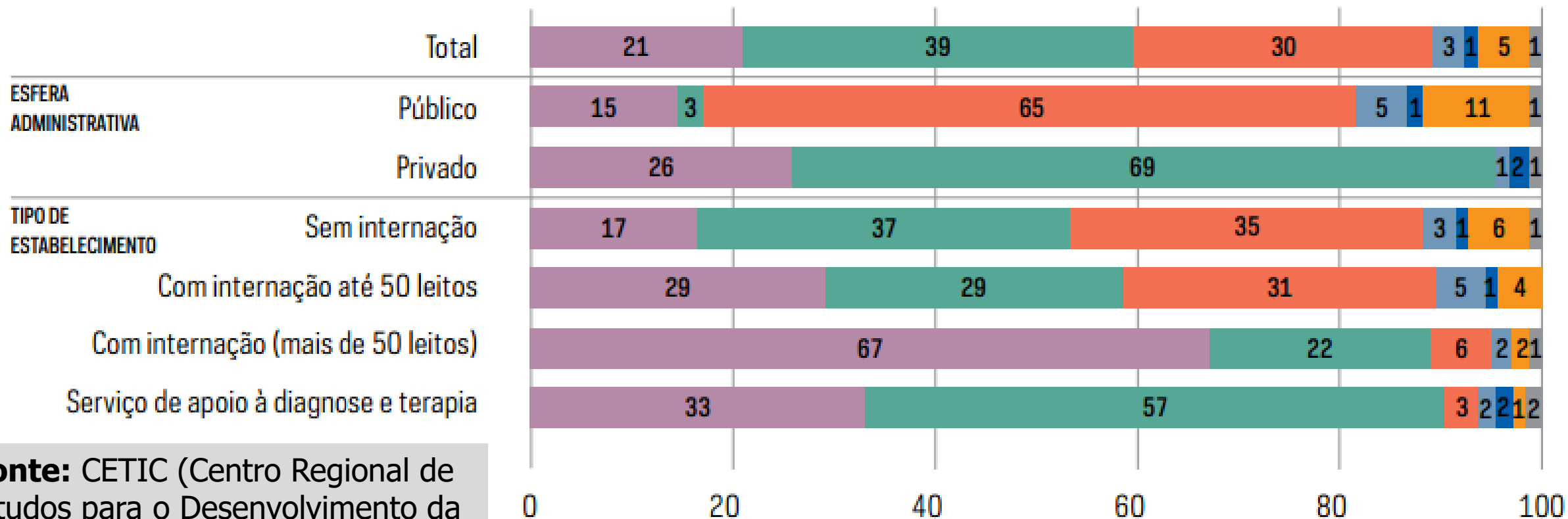


Usabilidade

- Sistemas de saúde baseados em cadeias de blocos → emprega **conceitos multidisciplinares** englobando...
 - Conhecimentos de **tecnologia da informação (TI)**
 - Competências e **fluxos de atendimento da área médica**
- **Principais Causas**
 - Baixa presença de profissionais qualificados
 - Alta complexidade de manipulação
- **Abordagens de Mitigação**
 - Criação de **interfaces intuitivas e habilitadas para quaisquer usuário**
 - Independente do nível de conhecimento técnico

Incorporação de *Blockchain* no Setor de Saúde

Equipe de TI em Estabelecimentos de Saúde



Fonte: CETIC (Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação)

- Equipe interna do estabelecimento
- Prestador de serviço contratado por outra instituição
- Prestador de serviço contratado pelo estabelecimento
- Voluntário
- Prestador de serviço contratado pela secretaria de saúde
- Outras organizações
- Não sabe/não respondeu

Irreversibilidade

- Relacionada à imutabilidade → propriedade intrínseca à cadeia de blocos
- **Casos Críticos**
 - **Registro de Dado Falsos ou Errados na *Blockchain***
 - Impossibilidade de exclusão ou correção do registro na cadeia de blocos
 - Nem mesmo pelos próprios autores ou por ordem judicial
 - **Necessidade de Armazenamento Temporário**
 - Impossibilidade de atualização de dados pessoais ou de procedimentos
 - Como **endereço residencial, estado civil...**
 - **Exposição de Chaves Privadas**
 - Não há como criptografar dados registrados novamente
 - Qualquer vazamento de chave **expõe permanentemente os dados do usuário**
 - Privacidade comprometida

Privacidade e Segurança

- Privacidade é naturalmente deficitária em cadeias de blocos
 - **Todos os nós acessam os dados transmitidos** por outro nó

Em casos emergenciais...

– Pacientes **dependem de uma entidade intermediadora**

- Para cessar suas próprias informações médicas → Rompe os princípios de privacidade
 - Estabelecidos nas legislações vigentes de proteção de dados: LGPD, HIPAA...

– Impactos Futuros

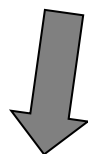
• **Computação Quântica**

- Promete resolver desafios criptográficos altamente complexos de maneira rápida e eficiente
 - Ao contrário dos computadores clássico → extremamente demorados
 - **Sérias ameaças à segurança da cadeia de blocos** baseada em criptografia de chave pública

Incorporação de Blockchain no Setor de Saúde

Desafios da Privacidade na Saúde Digital

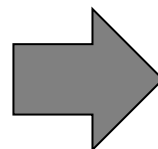
Disseminação da Internet das Coisas (IoT)



Aumento na **quantidade de dispositivos portáteis e vestíveis** usados nos cuidados digitais de saúde



Aumento na **necessidade de proteção da privacidade** dos usuários



Desafio
Encontrar equilíbrio entre...



Coleta de dados para fins de monitoramento



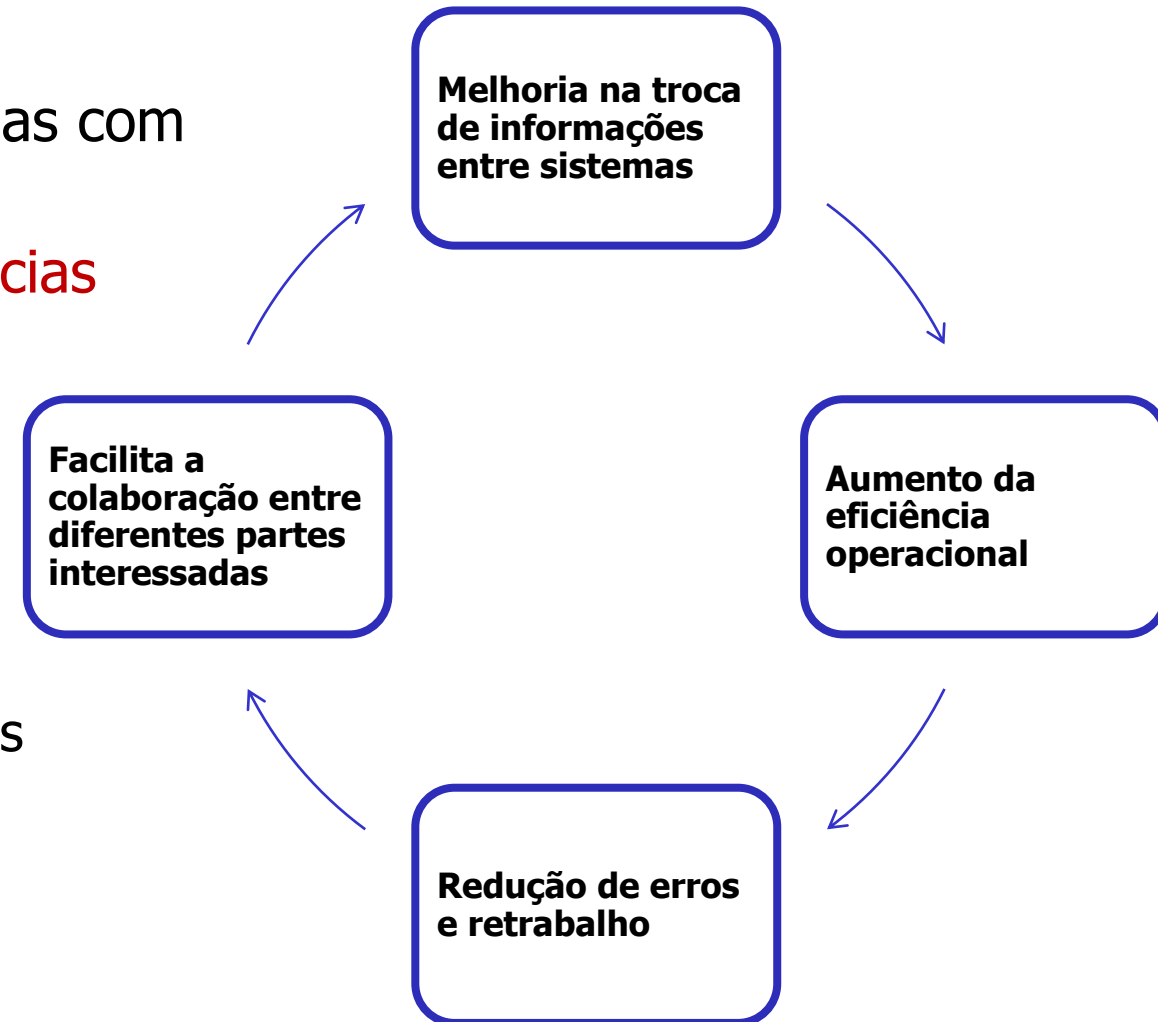
Respeito à privacidade dos usuários

Interoperabilidade

- Capacidade de trocar informações entre sistemas com características heterogêneas
- **Falta de Padronização dos Dados - Consequências**
 - Limita a capacidade de compartilhar os dados eletronicamente para o atendimento ao paciente

– Soluções

- Desenvolvimento de **novos padrões**
 - Que possam ser aderidos por soluções legadas



Interoperabilidade nos Sistemas de Saúde

Benefícios da Padronização



- **Melhoria na cooperação e coordenação entre os profissionais**
 - Informações trocadas de forma mais fácil e rápida mesmo com o uso de diferentes *softwares*
- **Redução do erro médico**
 - Com o compartilhamento de todo o histórico médico a probabilidade de um erro médico é menor com toda análise de dados do paciente
- **Transparência para o paciente**
 - Facilita o compartilhamento de registros médicos com os próprios pacientes

PROJETOS DE PESQUISA E DESENVOLVIMENTO



- **IHE** (*Integrating the Healthcare Enterprise*)
 - Iniciativa 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
 - Desenvolvendo perfis de integração com descrições de como diferentes padrões e especificações técnicas podem ser combinados para resolver problemas específicos de interoperabilidade

Sistemas de Saúde

CommonWell



- **CommonWell** é um projeto de pesquisa financiado pela União Europeia
 - Desenvolve 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

Project Information



CommonWell

Grant agreement ID: 225005



Closed project

Start date

1 October 2008

End date

31 January 2012

Funded under

Overall budget

€ 5 360 002,00


EU contribution

€ 2 680 000,00



Coordinated by

EMPIRICA GESELLSCHAFT FUR KOMMUNIKATIONS
UND TECHNOLOGIEFORSCHUNG MBH

 Germany

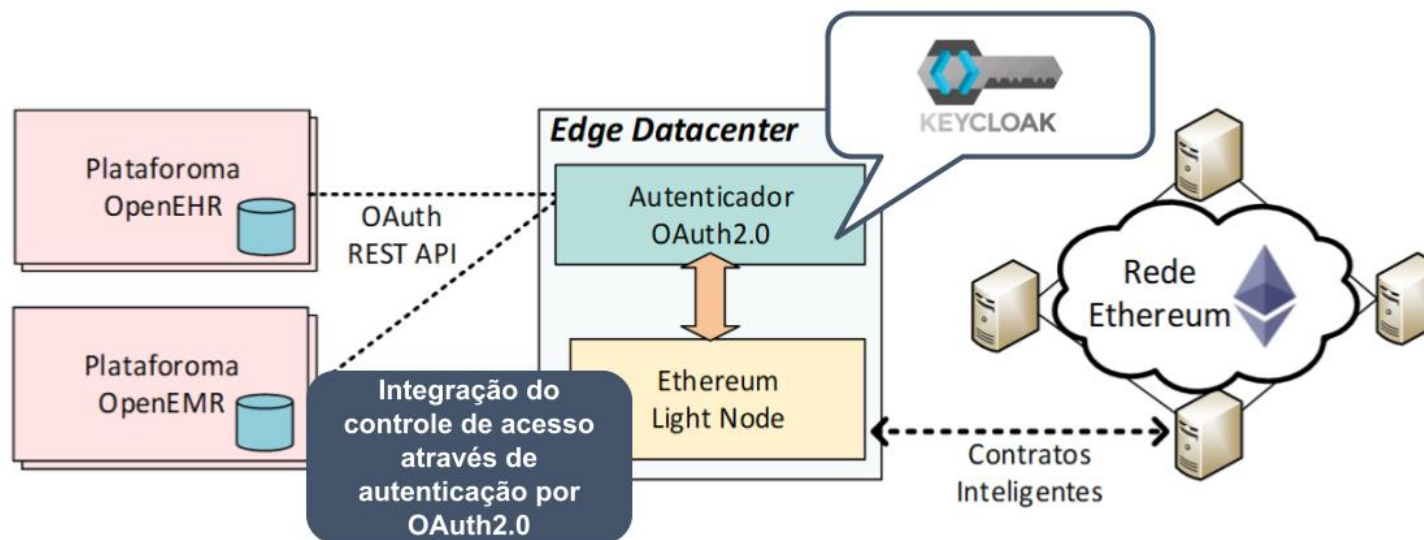
iDASH

- **iDASH** (Integrating Data for Analysis, Anonymization, and Sharing) é um projeto de pesquisa financiado pelo governo dos Estados Unidos para compartilhamento de dados seguramente
 - Desenvolve 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
 - Implementou medidas de segurança
 - E ajuda no compartilhamento e desenvolvimento de inovação

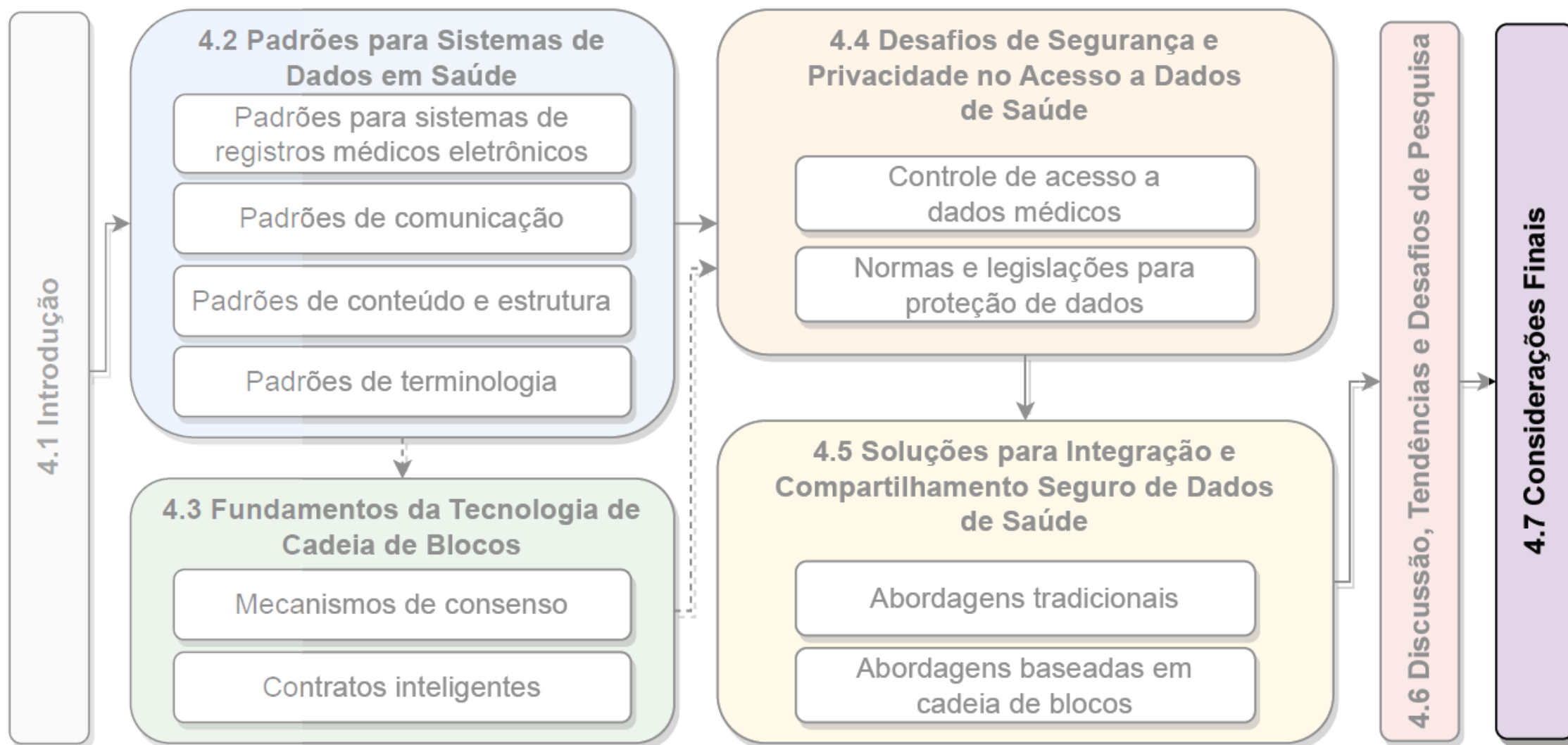


- **SmartMed** desenvolve um *software* de controle de acesso para sistemas de registros médicos eletrônicos
 - Surge para facilitar o acesso a múltiplos sistemas de saúde digital, permitindo o acesso seguro e ágil a informações armazenadas em bases não padronizadas e heterogêneas
 - Provê segurança e suporte na adequação dos sistemas de saúde à LGPD

- **SmartMed** é um software desenvolvido para aumentar a segurança para métodos informais e inseguros e adequar a LGPD
 - Dados médicos distribuídos com controle de acesso baseado em atributos através de contratos inteligentes
 - Cadeia de blocos com rede Ethereum e autenticação com Keycloak



Roteiro do Minicurso



- Papel Vital da Interoperabilidade nos Sistemas de Saúde
 - Rápida evolução da Tecnologia em Saúde (TIC)
 - Importância crescente de sistemas eletrônicos e plataformas digitais
 - Potencial
 - Revolucionar a prestação de cuidados de saúde
 - Melhorar o atendimento ao paciente
 - Desafio → **Complexidade e diversidade de formatos de dados dificultam a interoperabilidade**

- Registros Eletrônicos de Saúde (EHRs) e Compartilhamento Eficiente de Dados
 - Benefícios do **acesso rápido e padronizado** para atendimento integrado
 - Garantia de **privacidade e segurança** no compartilhamento de dados
 - Desafio → **Compartilhamento não autorizado e canais de comunicação informais**
- Importância do compartilhamento de dados
 - Registros dos pacientes
 - Iniciativas de saúde pública e detecção precoce de doenças
 - Melhoria da tomada de decisões e a continuidade do cuidado
 - Habilitação do acesso do paciente aos dados
 - Portabilidade entre provedores

- Papel da tecnologia Blockchain no futuro do sistemas de saúde
 - Desafios das arquiteturas cliente-servidor centralizadas
 - Padronização → fator chave para alcançar a interoperabilidade
 - Blockchain → **solução potencial para padronização e interoperação**
 - Desafios técnicos
 - **Escalabilidade, usabilidade, imutabilidade, privacidade, segurança, interoperabilidade**
- Benefícios da tecnologia Blockchain na área da saúde
 - Maior segurança e privacidade de dados → sistemas descentralizados e criptografados
 - Interoperabilidade → formatos de dados **padronizados** e contratos inteligentes
 - Pacientes com controle sobre seus dados de saúde
 - Gerenciamento de **consentimento**
 - Facilitação da **troca de dados segura e eficiente** entre os profissionais de saúde

Perspectivas Futuras

Colaboração na Inovação em Saúde



- Reconhecimento do mercado
 - Necessidade de interoperabilidade e segurança de dados
- Oportunidades
 - Projetos de pesquisa e produtos comerciais
- Padronizar e integrar sistemas de compartilhamento de registros médicos eletrônicos
 - Potencial para revolucionar a saúde e gerar resultados positivos para os pacientes

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 (TUDelft), Rafael Valle (RNP),
Dianne S. V. Medeiros (UFF), Diogo M. F. Mattos (UFF)