

Quando o dado precisa circular

Apostila do Encontro 3 — Sistemas de informação, terminologias,
interoperabilidade e segurança

Informática em Saúde Aplicada à Enfermagem

2026

Sumário

Apresentação	3
O que você deverá conseguir fazer	4
Como usar esta apostila	4
1. O problema que orienta o encontro	5
1.1 Caso Dona Celina	5
1.2 O percurso é maior que a transmissão	5
2. Conectividade, integração e interoperabilidade	6
2.1 Conectado não significa interoperável.....	6
2.2 Interoperabilidade semântica	7
2.3 Quatro camadas como instrumento de análise.....	7
Microatividade — diagnostique sem simplificar	8
3. Significado, contexto, qualidade e proveniência	8
3.1 Um valor não carrega sozinho a situação	8
3.2 Qualidade não é uma etiqueta única	9
Aplicação ao caso Celina	9
3.3 Proveniência: reconstruir origem e transformação	10
3.4 Corrigir na origem não encerra o problema	10
4. Terminologias e mapeamento semântico	11
4.1 Por que terminologias entram na conversa	11
4.2 LOINC: identificar observações e avaliações	11
4.3 SNOMED CT: representar conceitos clínicos	12
4.4 CIPE e ICNP no acervo processado	12
4.5 Terminologias se complementam.....	12
4.6 Mapeamento: a equivalência precisa ser examinada	13
5. RNDs: aprender pelas perguntas do percurso	14

5.1 Um roteiro funcional antes da especificação	14
6. Aprofundamento opcional: FHIR	15
6.1 O que as fontes permitem afirmar	15
6.2 Recurso: uma unidade modular	15
6.3 Uma API movimenta recursos	16
6.4 Tecnicamente válido ainda pode estar inadequado.....	16
6.5 Recurso, acordo e implementação	16
7. Segurança como propriedade do cuidado	17
7.1 Proteger não significa apenas esconder.....	17
7.2 Tríade CIA aplicada ao percurso	18
7.3 Privacidade e segurança: distinção operacional	19
7.4 Autenticação, autorização e auditoria	19
7.5 Proteger e permitir o trabalho	19
7.6 LGPD: cobertura geral e limite jurídico.....	20
7.7 Minimizar sem empobrecer o cuidado	20
8. Ameaças, controles e continuidade	21
8.1 Organizar o risco sem transformar o modelo em norma	21
8.2 Phishing: definição e controles	21
8.3 Ransomware e indisponibilidade	21
8.4 Bow-tie: barreiras antes e depois do evento	22
8.5 Controles precisam formar um conjunto	22
8.6 Interoperabilidade amplia dependências.....	23
8.7 Caso Celina: sistema indisponível.....	24
8.8 Desenhar uma contingência realista	24
9. Oficina integrada: um percurso auditável	25
9.1 Missão do grupo	25
9.2 Canvas integrado	25
9.3 Seis etapas em 70 minutos.....	25
9.4 Papéis para distribuir perspectivas	26
9.5 Entregável	26
9.6 Teste de qualidade antes de apresentar	27
9.7 Apresentação e crítica entre pares	27
10. Retorno ao caso Celina e síntese	28

10.1 O caso depois do percurso	28
10.2 Síntese visual.....	28
10.3 Três mensagens essenciais	28
10.4 Minuto de saída	29
11. Glossário comentado do Encontro 3	29
12. Atividades de consolidação	31
Atividade 1 — Autópsia de um dado que “chegou”	31
Atividade 2 — Qualidade situada	32
Atividade 3 — Auditoria de mapeamento	32
Atividade 4 — Sucesso técnico versus sucesso clínico	32
Atividade 5 — Bow-tie de indisponibilidade	33
Atividade 6 — Parecer de limites	33
13. Questões para discussão	33
14. Autoavaliação	34
Apêndice — Rastreabilidade.....	37
Matriz de rastreabilidade	37
Fontes citadas	42

Apresentação

Esta apostila acompanha exclusivamente o **Encontro 3** da disciplina **Informática em Saúde Aplicada à Enfermagem**. Foi escrita para estudantes de pós-graduação e parte de uma situação proposta para análise: um dado precisa sair de um ponto, chegar a outro e continuar suficientemente compreensível, confiável e disponível para apoiar uma decisão.

O encontro não é uma aula de engenharia de software. Seu foco é construir uma linguagem comum para analisar o percurso do dado. Em vez de começar por uma sigla ou por uma tecnologia, começaremos por perguntas: qual decisão precisa ser apoiada? Que dado deve circular? Quem o produz? Quem o recebe? Que significado precisa ser preservado? Como saber de onde ele veio? Quem pode acessá-lo? O que acontece quando o sistema falha?

Ideia central. Fazer os dados circularem não basta. Para apoiar o cuidado, eles precisam conservar significado, contexto, integridade, disponibilidade e proteção ao longo do percurso.

Essa tese será examinada por meio de um caso fictício, de explicações conceituais, de diagramas autorais e de uma oficina integrada. Nenhum caso apresentado constitui diagnóstico, protocolo assistencial, especificação técnica ou orientação jurídica.

O que você deverá conseguir fazer

Ao concluir o Encontro 3, espera-se que você consiga:

1. explicar, por meio do percurso de um dado, por que conexão e transporte não garantem significado compartilhado;
2. distinguir problemas predominantemente técnicos, estruturais, semânticos e organizacionais sem tratá-los como camadas isoladas;
3. analisar qualidade, contexto, atualidade, correção e proveniência de um dado em relação a uma decisão;
4. explicar como terminologias apoiam a comparação e o intercâmbio, reconhecendo que codificação não elimina contexto nem ambiguidade;
5. reconhecer os papéis descritos nas fontes para LOINC, SNOMED CT e ICNP no intercâmbio de dados;
6. explicar FHIR como uma abordagem baseada em recursos e tecnologias da Web, sem confundir sucesso técnico com adequação clínica;
7. analisar confidencialidade, integridade e disponibilidade como propriedades ligadas ao cuidado;
8. propor requisitos mínimos de acesso, correção, rastreabilidade, segurança e contingência para um percurso de dados;
9. comunicar um mapa de interoperabilidade e segurança a públicos clínicos, de pesquisa e técnicos.

Como usar esta apostila

O texto alterna explicações conceituais, casos hipotéticos, exemplos e atividades. Casos e exemplos que não correspondem a situações documentadas são identificados no próprio texto como fictícios ou didáticos; eles não constituem evidência científica, diagnóstico, protocolo assistencial nem orientação jurídica.

As chamadas numéricas entre colchetes funcionam como links para as referências documentais reunidas em **Fontes citadas**, ao final do documento. A repetição de um número indica o emprego da mesma fonte, página e trecho. Quando o acervo não oferece base suficiente para uma definição ou afirmação, o limite é registrado explicitamente no texto.

1. O problema que orienta o encontro

1.1 Caso Dona Celina

Caso hipotético.

Celina, 72 anos, vive com diabetes e doença renal crônica. Durante uma transferência entre serviços, uma medida de glicemia aparece em unidades diferentes, a informação de alergia está registrada em texto livre, parte do histórico chega em um arquivo PDF e uma observação de enfermagem não é incorporada ao resumo recebido pela equipe.

A situação produz uma pergunta desconfortável: **a informação chegou ou apenas uma nova incerteza foi transportada?**

Não tente resolver o caso clinicamente. Primeiro, decomponha o problema. Há pelo menos cinco possibilidades de falha:

1. um dado necessário não chegou;
2. um dado chegou, mas foi interpretado de maneira diferente;
3. um dado estava desatualizado;
4. um dado correto não ficou disponível no momento necessário;
5. um dado foi exposto ou acessado fora das condições previstas.

Para refletir. Escolha a falha que você investigaria primeiro e escreva uma frase justificando sua prioridade. Guarde a resposta. Ela será retomada no final do encontro.

1.2 O percurso é maior que a transmissão

O prontuário eletrônico é descrito como um registro longitudinal que reúne informações produzidas em um ou mais encontros de cuidado, apoia o workflow e pode sustentar comunicação, decisão, gestão da qualidade e relatórios. A definição também associa o EHR à possibilidade de consulta por profissionais autorizados além de uma única organização [1] [2].

Entretanto, reunir ou transmitir registros não elimina diferenças entre instituições. As fontes descrevem dados ausentes, informações mantidas apenas em papel, dados produzidos fora da organização e diferenças de representação decorrentes de fornecedores, configurações locais, regras de negócio e códigos distintos [3].

Por isso, a circulação precisa ser analisada como um percurso:

Origem → registro → estrutura → transmissão → interpretação → incorporação ao trabalho → decisão → correção ou reavaliação.

Aplicação ao caso. Cada seta representa uma passagem que pode preservar, transformar, ocultar ou perder informação. O arquivo recebido pode estar tecnicamente íntegro e ainda

ser insuficiente para a tarefa. Um campo pode ser reconhecido pelo sistema receptor, mas permanecer ambíguo para quem decide. Uma informação correta pode chegar depois do momento em que seria útil [3] [4].

Aplicação ao caso. No caso Celina, a pergunta central não é “os sistemas estão conectados?”. A pergunta é “o percurso permite que a equipe reconstrua o que foi observado, em que condições, por quem, quando, como foi transformado e para que decisão pode ser usado?”.

2. Conectividade, integração e interoperabilidade

2.1 Conectado não significa interoperável

A fonte sobre prontuário eletrônico afirma explicitamente que melhorias de conectividade, isoladamente, não são suficientes para produzir um registro longitudinal. Ela acrescenta interoperabilidade, comparabilidade, apoio à decisão e captura de dados no ponto de cuidado como componentes necessários [5].

Essa distinção merece ser lida lentamente. **Conectividade** responde se existe um caminho técnico entre pontos. **Transporte** responde se um arquivo, mensagem ou conjunto de campos foi enviado. **Integração**, nesta apostila, será usada como rótulo pedagógico para a incorporação do dado a outro sistema ou fluxo. **Interoperabilidade semântica** exige que a troca não provoque perda de contexto ou significado e que o dado possa ser reutilizado sem esforço especial do usuário [4].

Situação observada	O que foi alcançado	O que ainda precisa ser demonstrado
a rede funciona	conectividade	se o conteúdo será transmitido e reconhecido
o arquivo foi enviado	transporte	se a estrutura permite localizar os elementos
os campos foram importados	reconhecimento estrutural	se o significado e o contexto foram preservados
o dado aparece na tela	disponibilidade visual	se participa do trabalho no momento certo
o dado foi usado	incorporação ao processo	se a interpretação e a decisão foram adequadas

A tabela é uma comparação operacional, não uma taxonomia universal. Uma mesma falha pode atravessar várias linhas.

2.2 Interoperabilidade semântica

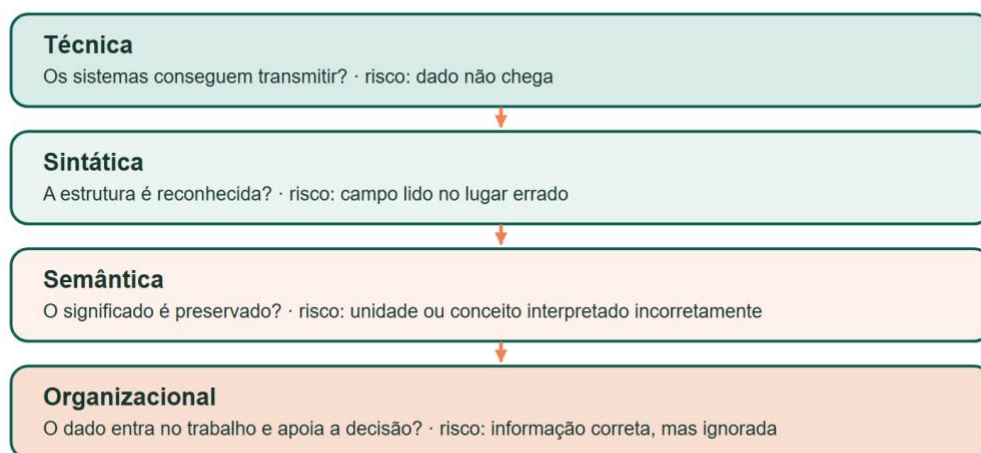
A interoperabilidade semântica é definida na fonte como troca de dados sem perda de contexto ou significado, permitindo reutilização sem esforço especial por parte do usuário. Para isso, a fonte relaciona conteúdo clínico padronizado, taxonomias ou vocabulários para codificação e padrões de mensagem para transporte entre organizações. Ela também destaca que códigos, atributos e estruturas de dados precisam representar o elemento completo, e não apenas um rótulo isolado [4].

Caso para análise. Considere a palavra “alergia”. Isoladamente, ela não informa qual substância está envolvida, que manifestação foi observada, quando o registro foi produzido, quem o confirmou nem se houve atualização. Um sistema pode transportar corretamente a palavra e, ainda assim, deixar o receptor sem elementos suficientes para interpretar o caso.

Em conjunto, as fontes citadas indicam que interoperar exige articular pelo menos três objetos: uma estrutura que organize o dado, um vocabulário que represente o conceito e um processo capaz de usar e corrigir a informação. Padrões ajudam a reduzir diferenças, mas as fontes também documentam regras locais, códigos distintos, ausência de vocabulário comum e necessidade de atualização em todos os sistemas receptores quando um erro é descoberto [3] [6] [7].

2.3 Quatro camadas como instrumento de análise

Interoperabilidade: camadas que se combinam



Não é uma escada rígida: uma implementação pode falhar em mais de uma camada.

Quatro camadas pedagógicas para analisar interoperabilidade

O diagrama organiza quatro perguntas. Ele não deve ser tratado como escada rígida nem como classificação normativa validada.

1. **Técnica — o dado consegue chegar?** Examine rede, transmissão, autenticação entre componentes e disponibilidade dos serviços.

2. **Sintática — a estrutura é reconhecida?** Examine campos, formatos, mensagens, unidades e posições esperadas.
3. **Semântica — emissor e receptor preservam o significado?** Examine conceitos, códigos, atributos, contexto e transformações.
4. **Organizacional — o dado entra no trabalho?** Examine papéis, tempo, responsabilidades, correção, comunicação e decisão.

A camada semântica possui apoio conceitual direto nas fontes. As demais são uma organização pedagógica inspirada nos problemas de conectividade, representação, workflow e responsabilidade documentados nos capítulos processados [4] [3] [7].

Microatividade — diagnostique sem simplificar

Associe cada situação a uma camada predominante e indique uma segunda camada envolvida.

1. um resultado não chega ao sistema receptor;
2. um campo é importado como texto e não pode ser usado em cálculo;
3. um código é associado a um conceito diferente no sistema receptor;
4. um alerta correto aparece depois que a decisão já foi tomada.

Não procure uma resposta única. O primeiro caso parece técnico, mas pode envolver uma regra organizacional de envio. O segundo parece estrutural, mas afeta o significado operacional. O quarto parece organizacional, mas pode resultar da configuração técnica de atualização.

3. Significado, contexto, qualidade e proveniência

3.1 Um valor não carrega sozinho a situação

Exemplo didático.

Valor: 220 Unidade: mg/dL
Material: capilar Método: glicosímetro
Horário: 08:15 Condição: após alimentação
Pessoa: identificada
Dispositivo e responsável: identificados

Interpretação. O exemplo não orienta conduta. Ele serve para mostrar que um número ganha capacidade de interpretação quando é relacionado a unidade, material, método, tempo, condição, identidade e origem. A pergunta correta não é “o dado está completo em termos absolutos?”, mas “o conjunto disponível é suficiente para a decisão pretendida?”.

As fontes mostram que diferenças locais nos identificadores de observações e nos valores codificados dificultam integrar dados de organizações distintas. Também registram o uso de padrões para observações, unidades e conceitos, precisamente porque um valor isolado não resolve a diversidade de representações [8].

3.2 Qualidade não é uma etiqueta única

Os capítulos processados associam integridade a precisão e completude, documentam erros de entrada e transferência, destacam a necessidade de manter dados atuais e mostram que conteúdo copiado pode permanecer desatualizado ou perder contexto [9] [10] [11].

Transforme “qualidade” em seis perguntas operacionais:

Dimensão didática	Pergunta
presença	os elementos necessários foram registrados?
unicidade	existem duplicações ou versões concorrentes?
validade	valor, formato e relação entre campos são admissíveis?
consistência	diferentes partes do percurso contam a mesma história?
atualidade	o dado representa o estado relevante para este momento?
adequação ao uso	o conjunto permite a interpretação necessária para a decisão?

Essa organização tem finalidade didática; não é um instrumento validado. Sua finalidade é impedir frases genéricas como “o banco é bom” ou “o dado é ruim” sem explicitar o uso, a falha e a consequência.

Aplicação ao caso Celina

Avalie separadamente a glicemia, a alergia, o PDF e a observação de enfermagem.

- A glicemia pode estar presente, mas com unidade ou contexto divergente.
- A alergia pode estar presente, mas ambígua por permanecer em texto livre.
- O PDF pode estar disponível, mas exigir busca manual e ocultar elementos estruturados.
- A observação de enfermagem pode ser válida na origem e ainda assim estar ausente no resumo receptor.

Essas possibilidades são inferências do caso fictício. Elas não afirmam que todo texto livre, PDF ou resumo produz necessariamente falha.

3.3 Proveniência: reconstruir origem e transformação

A especificação FHIR R4B define a proveniência de um recurso como o registro das entidades e dos processos que participaram de sua produção, entrega ou influência. O recurso Provenance acompanha atividades de criação, revisão, exclusão ou assinatura e os agentes e entidades envolvidos [12]. A recomendação PROV-O do W3C fornece classes, propriedades e restrições para representar e intercambiar informação de proveniência entre sistemas e contextos [13].

As fontes de prontuário complementam essa definição com mecanismos concretos: trilhas de auditoria capazes de mostrar quem inseriu ou alterou um dado; registro de data, hora e identidade do usuário; políticas de correção; manutenção de dicionários; e atualização dos sistemas que receberam uma informação incorreta [7] [14].

Para fins didáticos. Nesta apostila, a ficha de proveniência traduz esses conceitos para a reconstrução da origem e das transformações relevantes de um dado; ela não constitui um modelo universal de qualidade.

Ficha de proveniência. Para cada elemento, registre:

- sistema, pessoa ou dispositivo de origem;
- autor ou responsável pelo registro;
- data e hora;
- transformação ou conversão realizada;
- versão ou estado conhecido;
- correção posterior e sistemas que precisam recebê-la.

Um dado pode estar correto e ainda ser inadequado para um uso se sua transformação ou sua atualização não puder ser reconstruída. Essa frase é uma aplicação ao caso a partir dos mecanismos de auditoria, correção e atualização descritos nas fontes [7].

3.4 Corrigir na origem não encerra o problema

Quando um erro é descoberto, a fonte afirma que a informação precisa ser corrigida no sistema inicial e nos sistemas receptores que dela derivam dados. A atualização pode ocorrer por transações de interface ou por intervenção manual. A mesma fonte relaciona trilhas de auditoria ao acompanhamento de quem inseriu ou modificou cada elemento [7].

Aplicação ao caso. Quanto maior o número de destinos, maior a necessidade de saber onde o dado foi replicado, transformado ou usado. A correção não é apenas uma edição local. Ela é um processo de propagação, verificação e responsabilização [7].

Para refletir. Se a alergia de Celina for corrigida na origem, quem identifica todos os destinos, quem confirma a atualização e que evidência demonstra que uma versão incorreta deixou de orientar o trabalho?

4. Terminologias e mapeamento semântico

4.1 Por que terminologias entram na conversa

Diferenças locais de nomes e códigos constituem barreira importante à integração de registros. As fontes descrevem terminologias padronizadas para representar observações, diagnósticos, sintomas, achados, unidades e medicamentos. Também afirmam que a padronização de termos clínicos facilita entendimento comum, comparação de resultados, comunicação entre disciplinas e análise das contribuições da enfermagem [8] [15].

Uma terminologia não é apenas uma lista de palavras “corretas”. Ela oferece identificadores e relações que ajudam sistemas e pessoas a reconhecer conceitos de modo compartilhado e a relacioná-los ao intercâmbio [15] [4].

Ao mesmo tempo, codificar não elimina a necessidade de contexto. A fonte sobre interoperabilidade semântica inclui atributos e estruturas de dados na representação do elemento completo. Portanto, o código precisa ser lido junto com os demais componentes necessários ao caso de uso [4].

Tensão produtiva. Padronizar pode tornar o cuidado comparável e analisável; uma escolha estreita de termos também pode reduzir nuances. A tarefa não é escolher entre padronização e narrativa, mas justificar o que precisa ser estruturado, o que precisa ser descrito e como as duas formas serão relacionadas.

4.2 LOINC: identificar observações e avaliações

A fonte descreve LOINC como terminologia usada para observações, perguntas, variáveis e avaliações. Outro capítulo o apresenta como sistema universal de códigos para identificar observações laboratoriais e outras observações clínicas [8] [16].

Síntese didática: LOINC ajuda a responder: **qual observação, medida, pergunta ou avaliação está sendo identificada?** O código não substitui o resultado, a unidade, o método, o tempo nem o contexto. Identificar o tipo de observação não equivale a registrar todas as condições que permitem interpretá-la [8] [4].

Não procure um código real durante a atividade. Escreva primeiro uma descrição completa da observação de Celina e destaque os componentes que não podem ser perdidos no

intercâmbio. Consulta a códigos e versões oficiais somente deve ocorrer em uma etapa posterior, com fonte normativa apropriada.

As notas de versão incorporadas ao corpus registram o lançamento do LOINC 2.82 em fevereiro de 2026 e documentam alterações e totais de conceitos, mas não fornecem a seleção de códigos necessária ao caso Celina [17].

4.3 SNOMED CT: representar conceitos clínicos

A fonte associa SNOMED CT a diagnósticos, sintomas, achados, organismos e respostas. Outro capítulo relata sua adoção como terminologia clínica padronizada para prontuários eletrônicos [8] [18].

Sua função no percurso é diferente da função de uma terminologia voltada a identificar observações. O uso documentado nas fontes reforça que terminologias podem ocupar papéis complementares. Uma observação pode exigir um identificador para o que foi medido, uma unidade computável e conceitos adicionais para representar achados ou respostas [8].

Limite. Granularidade, seleção do conceito, contexto e versão devem permanecer como questões explícitas de governança. Não trate a existência de um código como prova de equivalência completa.

4.4 CIPE e ICNP no acervo processado

O roteiro da aula nomeia este tópico como CIPE. As fontes empregam a sigla **ICNP** e a descrevem como linguagem comum de códigos para dados de enfermagem e como terminologia composicional para diagnósticos, ações e resultados, representada por sete eixos e utilizável tanto no ponto de cuidado quanto como terminologia de referência [19] [20].

Informação não identificada nas fontes fornecidas: correspondência normativa brasileira entre as siglas CIPE e ICNP, versão vigente e estrutura atual da classificação. A fonte localizada descreve a versão 2.0, publicada em 2009, e por isso não sustenta afirmações sobre a versão atual.

Para esta aula, a contribuição conceitual sustentada é mais restrita: uma linguagem comum de códigos pode favorecer intercâmbio de dados de enfermagem preservando significado. Não se deve transformar esse trecho em orientação de codificação ou afirmação sobre uma versão vigente sem documentação oficial adicional [19].

4.5 Terminologias se complementam

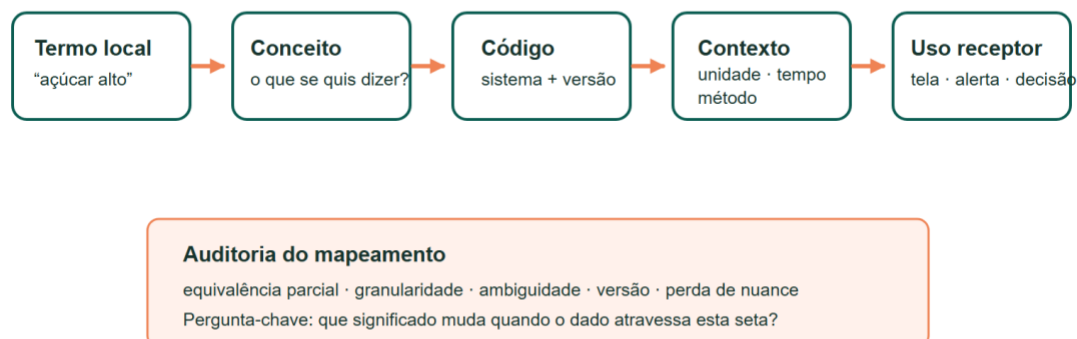
As fontes mostram que terminologias distintas podem cumprir papéis complementares na identificação de observações, conceitos clínicos e dados de enfermagem [8] [19].

Necessidade no percurso	Sistema terminológico descrito nas fontes	Pergunta didática
identificar observação, pergunta, variável ou avaliação	LOINC	o que foi observado ou avaliado?
representar diagnóstico, sintoma, achado, organismo ou resposta	SNOMED CT	que conceito clínico precisa ser reconhecido?
intercambiar dados de enfermagem preservando significado	ICNP, conforme denominação da fonte	que elemento de enfermagem precisa permanecer compreensível?

A escolha depende do caso de uso e do tipo de dado. As fontes também apresentam UCUM para unidades computáveis e RxNorm para nomes e componentes de medicamentos, mostrando que um percurso pode mobilizar diferentes padrões simultaneamente [8].

4.6 Mapeamento: a equivalência precisa ser examinada

Mapear não é apenas substituir palavras



Fluxo pedagógico do termo local ao uso receptor

Sistemas de integração podem traduzir formatos e códigos durante o intercâmbio. As fontes também descrevem mapeamentos construídos entre categorias de problemas, observações e medicamentos, com uso de terminologias padronizadas [21] [22].

Para fins didáticos. Mapear não é apenas substituir uma palavra por outra. É declarar uma relação entre uma expressão local, um conceito selecionado, um código, os atributos necessários e o modo como o receptor usará a informação. Essa relação pode ser incompleta, incerta ou dependente do contexto.

Auditoria rápida. Para o termo local “alergia forte”, registre:

1. o conceito que o autor provavelmente tentou expressar;
2. a informação que está ausente;
3. a possível perda se o termo for convertido automaticamente;
4. a pergunta que precisa voltar ao autor ou responsável;
5. a maneira de manter a incerteza visível até a confirmação.

Não procure um código. O objetivo é reconhecer ambiguidade antes da codificação.

5. RNDS: aprender pelas perguntas do percurso

O conteúdo processado sustenta a importância de registros que atravessem mais de uma organização, de padrões de intercâmbio e de redes de troca de informação. Também mostra que prontuários longitudinais dependem de interoperabilidade, vocabulários, regras e acesso autorizado [1] [6].

Uma página do guia da RNDS agora incorporada ao corpus descreve a integração de resultados laboratoriais para COVID-19 e Monkeypox e afirma que o compartilhamento permite acesso por profissionais para continuidade do cuidado e pelos próprios cidadãos. A própria página limita seu escopo a esses resultados laboratoriais [23].

Informação não identificada nas fontes fornecidas: arquitetura completa, conjunto de serviços e documentos clínicos, regras de acesso, governança e especificações vigentes da RNDS. A apostila, portanto, não extrapolará a página localizada para descrever componentes ou obrigações de toda a rede.

5.1 Um roteiro funcional antes da especificação

Ao encontrar a sigla RNDS em um projeto, não comece desenhando a tecnologia. Registre as perguntas que precisarão ser respondidas por documentação oficial e governança competente:

1. que dado precisa circular e para qual decisão;
2. quem produz, envia, recebe, usa e corrige;
3. que significado, contexto e proveniência precisam acompanhar o dado;
4. que padrão, terminologia, versão e regras de validação serão exigidos;
5. quem pode acessar, em quais condições e com que registro de auditoria;
6. como indisponibilidade, correção e reconciliação serão tratadas;
7. que evidência demonstrará que o percurso funcionou para o uso pretendido.

O roteiro tem finalidade didática. Ele não substitui documentação técnica, normativa ou institucional.

6. Aprofundamento opcional: FHIR

Este bloco é um aprofundamento opcional do Encontro 3. Ele deve ser utilizado quando o projeto realmente exigir uma primeira aproximação técnica. O objetivo não é programar nem produzir uma especificação implementável, mas compreender por que uma estrutura de intercâmbio não resolve sozinha significado, qualidade e processo.

6.1 O que as fontes permitem afirmar

As fontes apresentam FHIR como um padrão da HL7 voltado à Web. Ele se apoia em tecnologias e métodos comuns da Web, incluindo XML, JSON, HTTP e OAuth, e organiza a interoperabilidade por meio de **recursos**, descritos como unidades básicas e componentes modulares [24] [25].

Outro capítulo descreve FHIR como uma interface de programação para troca de dados clínicos e registra sua relação com aplicativos capazes de acessar dados de prontuários por mecanismos padronizados [26].

Essas descrições ajudam a separar duas ideias:

- **estrutura modular:** o intercâmbio é organizado em unidades que podem ser relacionadas;
- **acesso padronizado:** aplicações podem solicitar, inserir ou atualizar dados por uma interface definida.

Aplicação ao caso. Essas descrições não autorizam concluir que qualquer implementação FHIR preserve automaticamente significado clínico, contexto, integridade ou adequação ao trabalho [24] [4].

6.2 Recurso: uma unidade modular

A fonte define recursos como unidades básicas de interoperabilidade e componentes modulares que podem ser combinados em sistemas voltados a problemas clínicos, administrativos e de infraestrutura [25].

Um segundo exemplo documentado é o recurso **Questionnaire**, destinado à captura de dados por formulários e capaz de representar lógica de salto, agrupamentos e verificações simples [27].

Exemplo didático. Pense no recurso como uma unidade estruturada do intercâmbio, não como uma ficha completa da pessoa. O valor aparece quando a unidade é relacionada a outras informações, a terminologias, a regras e ao processo que a utiliza. A analogia é didática e não substitui a definição oficial do padrão.

Informação não identificada nas fontes fornecidas: lista oficial atual de tipos de recurso, cardinalidades, elementos obrigatórios, perfis nacionais, extensões e regras de validação vigentes.

6.3 Uma API movimenta recursos

As fontes descrevem o acesso a recursos FHIR por uma API RESTful baseada em requisições HTTP para **GET, PUT, POST e DELETE** dados [24] [25].

Didaticamente, esses verbos podem ser lidos como operações de consultar, criar, atualizar ou remover representações. Não é necessário executar uma chamada. O ponto conceitual é mais importante: **o sucesso técnico de uma requisição informa que uma operação ocorreu; não demonstra que o conteúdo está completo, atual, semanticamente equivalente ou adequado à decisão**. Essa conclusão é uma síntese entre a descrição técnica de FHIR e os problemas de integridade, representação e interoperabilidade semântica documentados nas fontes [24] [4] [10].

6.4 Tecnicamente válido ainda pode estar inadequado

Como usar a matriz. Percorra cinco perguntas em ordem, sem tratar a sequência como modelo normativo.

Verificação	Pergunta de revisão
estrutura	a unidade enviada possui a forma esperada?
acordo de uso	emissor e receptor seguem a mesma especificação para este percurso?
terminologia	conceito, código, atributos e versão são compatíveis?
semântica	o receptor interpreta a informação como o emissor pretendia?
processo	o dado apoia a pessoa certa, na tarefa e no momento necessários?

Aplicação ao caso. Uma mensagem pode ser aceita pelo sistema e ainda carregar um texto ambíguo. Um código pode ser reconhecido e estar associado a contexto insuficiente. Um recurso pode chegar depois da decisão. A matriz serve para manter essas possibilidades visíveis.

6.5 Recurso, acordo e implementação

Para esta aula, utilize três níveis de conversa:

1. **Recurso:** qual unidade estruturada representa parte do dado?

2. **Acordo de uso:** que restrições, terminologias e regras emissor e receptor precisam compartilhar?
3. **Implementação:** como pessoas, sistemas, testes, correções e contingências tornam o acordo operacional?

O primeiro nível possui apoio direto nas fontes. Os dois seguintes são uma organização didática para evitar que o padrão seja confundido com uma implementação completa [25].

A especificação FHIR R4 define perfil como um conjunto de restrições sobre um recurso representado por uma StructureDefinition e descreve um guia de implementação como um conjunto coerente e delimitado de adaptações publicado como unidade [28]. A mesma versão apresenta extensibilidade como parte fundamental do desenho: elementos podem conter extensões para representar requisitos adicionais, submetidas a regras de definição e uso; no elemento Extension, a URL tem cardinalidade 1..1 e o valor, 0..1 [29] [30].

Esses documentos são páginas da versão R4 e informam que existe versão posterior. Informação não identificada nas fontes fornecidas quanto aos perfis nacionais aplicáveis ao caso, às cardinalidades dos recursos selecionados e ao guia de implementação vigente que deveria reger uma implementação brasileira.

Regra de estudo: se o projeto exigir especificação técnica, interrompa a inferência e consulte a versão oficial aplicável. A apostila oferece vocabulário para formular perguntas, não uma configuração pronta.

7. Segurança como propriedade do cuidado

7.1 Proteger não significa apenas esconder

O prontuário eletrônico é descrito como sistema que deve apoiar confidencialidade, privacidade, trilhas de auditoria e acesso contínuo por usuários autorizados [31].

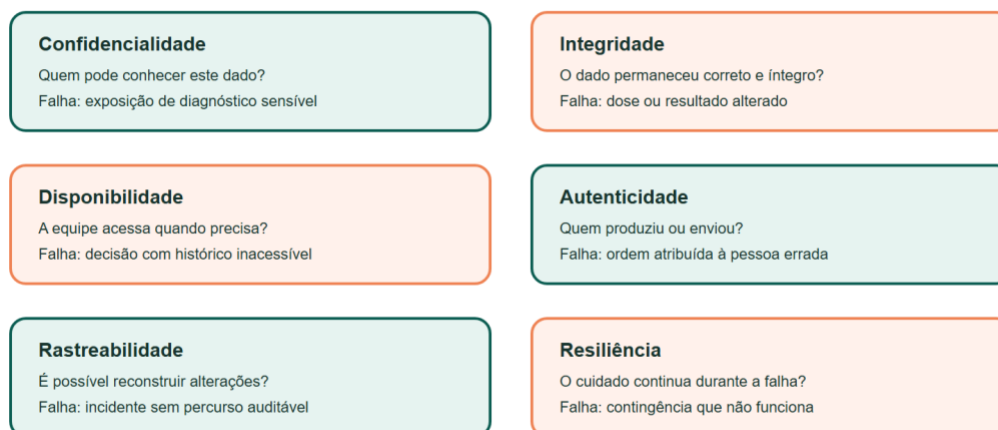
A integridade dos dados pode ser comprometida por entrada incorreta, adulteração ou falha do sistema. A fonte associa sua preservação a medidas de segurança, trilhas de auditoria, políticas e procedimentos, além de enfatizar que a exatidão depende das pessoas que registram e dos sistemas que transferem os dados [10].

A disponibilidade também possui consequência assistencial. Manutenção e falhas podem exigir formulários em papel, comunicação alternativa, verificação posterior, entrada manual e reconciliação do conteúdo produzido durante a indisponibilidade. As fontes recomendam procedimentos de downtime e recuperação com papéis e responsabilidades definidos [32].

Em conjunto, as fontes citadas indicam que segurança não é uma propriedade separada do cuidado. Acesso indevido, dado alterado e dado indisponível produzem problemas diferentes, mas todos podem comprometer o uso clínico da informação [31] [10] [32].

7.2 Tríade CIA aplicada ao percurso

Segurança protege o cuidado — não apenas o servidor



Segurança analisada a partir de consequências para o cuidado

Leia a tríade CIA como três perguntas ligadas ao trabalho:

Propriedade	Pergunta operacional	Falha possível no caso Celina
confidencialidade	somente pessoas autorizadas acessam o dado nas condições previstas?	exposição da informação por canal inadequado
integridade	o dado permanece correto e as alterações podem ser reconstruídas?	alergia corrigida em um sistema e antiga em outro
disponibilidade	o dado pode ser acessado no momento necessário?	prontuário indisponível durante a transferência

A fonte sustenta acesso autorizado, confidencialidade, integridade, auditoria, disponibilidade contínua e procedimentos para falha. A organização em perguntas e o exemplo têm finalidade didática [31] [10] [32].

O diagrama acrescenta autenticidade, rastreabilidade e resiliência como lentes de análise. Elas não são apresentadas aqui como uma extensão normativa da tríade. Servem para perguntar quem produziu o dado, como o percurso pode ser auditado e como o serviço continua e se recupera diante de falhas.

7.3 Privacidade e segurança: distinção operacional

As fontes relacionam privacidade ao dever de preservar as condições de acesso e compartilhamento das informações da pessoa. Também descrevem mecanismos de segurança como autenticação, controle de acesso, criptografia, firewalls e trilhas de auditoria [33] [34].

Distinção para análise.

- **privacidade:** por que, para que, por quem e sob quais condições a informação será tratada;
- **segurança:** que salvaguardas protegem acesso, integridade, disponibilidade e responsabilização.

Essa distinção é operacional e não constitui definição jurídica. Ela ajuda a perceber por que uma informação pode estar tecnicamente protegida e ainda ser usada para finalidade inadequada, ou ser necessária ao cuidado e permanecer indisponível por um controle mal desenhado.

7.4 Autenticação, autorização e auditoria

O sistema precisa reconhecer a identidade do usuário e limitar acesso a pessoas autorizadas. As fontes descrevem identificação por credenciais, autenticação, controles de acesso e trilhas capazes de registrar data, hora, identidade e alteração realizada [33] [14].

Esses mecanismos respondem a perguntas distintas:

- **autenticar:** quem está tentando acessar ou registrar?
- **autorizar:** essa identidade pode realizar esta ação neste contexto?
- **auditar:** que ação ocorreu, quando, sobre qual informação e por qual identidade?

Síntese didática: autenticação não substitui autorização, e ambas não substituem auditoria. Reconhecer a identidade não prova que a ação era apropriada; permitir uma ação não elimina a necessidade de registrá-la e revisá-la [33] [14].

7.5 Proteger e permitir o trabalho

A fonte registra uma relação inversa entre facilidade de acesso e robustez da segurança e afirma que sistemas de informação em saúde precisam equilibrar restrição, realização do trabalho e responsabilização. Também recomenda políticas, treinamento, detecção de intrusão, controles de acesso e trilhas de auditoria [35].

Síntese didática: isso não significa enfraquecer segurança para ganhar velocidade. Significa testar se o controle protege a informação sem criar bloqueios indevidos, atrasos, atalhos informais ou perda de continuidade. A resposta é analisar o arranjo entre tecnologia, política, tarefa, treinamento e condições de trabalho [35].

Para refletir. Que controle protege o dado, mas pode atrasar o cuidado quando mal desenhado? Como manter a proteção e reduzir o efeito adverso?

7.6 LGPD: cobertura geral e limite jurídico

O texto compilado da LGPD incorporado ao corpus classifica dados referentes à saúde, dados genéticos e biométricos vinculados a uma pessoa como dados pessoais sensíveis [36]. Ele também estabelece princípios de finalidade, adequação, necessidade, livre acesso, qualidade, transparência e segurança e apresenta hipóteses legais distintas para o tratamento, incluindo estudos por órgão de pesquisa, proteção da vida e tutela da saúde [37] [38].

Informação não identificada nas fontes fornecidas: interpretação jurídica e aplicação específica desses dispositivos ao caso desta apostila.

Esta apostila não apresenta interpretação jurídica. Não conclua que consentimento é sempre necessário ou suficiente e não use os capítulos estrangeiros disponíveis como substitutos da legislação brasileira.

Roteiro de trabalho.

1. que dados e finalidades estão envolvidos;
2. que itens precisam ser verificados como dados pessoais ou sensíveis;
3. qual necessidade e qual base jurídica precisam ser confirmadas;
4. quem são os atores e responsáveis pelo tratamento;
5. que direitos e procedimentos devem ser observados;
6. que controles, registros e respostas a incidentes são exigidos.

O roteiro apenas organiza perguntas. As respostas dependem de fonte oficial vigente e de apoio institucional competente.

7.7 Minimizar sem empobrecer o cuidado

Formule a pergunta completa: **qual é o conjunto mínimo necessário — e mínimo para qual decisão?**

No caso Celina, retirar uma informação essencial do resumo pode reduzir exposição e, simultaneamente, produzir perda de contexto assistencial. Compartilhar tudo, sem finalidade e sem controle, também não resolve o problema. O exercício consiste em justificar finalidade, conteúdo, acesso, tempo de disponibilidade e responsabilidade de correção sem formular conclusão legal.

8. Ameaças, controles e continuidade

8.1 Organizar o risco sem transformar o modelo em norma

Cadeia de análise.

ativo → vulnerabilidade → ameaça → evento → consequência

Distinção para análise. O **ativo** é aquilo que precisa ser protegido ou mantido disponível. A **vulnerabilidade**, nesta atividade, é uma condição que pode favorecer falha ou uso indevido. A **ameaça** é uma possibilidade de exploração ou dano. O **evento** é o que efetivamente ocorre. A **consequência** descreve o efeito sobre informação, trabalho ou cuidado.

Essa cadeia é um organizador pedagógico, não uma taxonomia normativa. Sua função é impedir que palavras como “ataque”, “risco” e “falha” sejam usadas como sinônimos.

Exemplo didático. Use “credencial compartilhada” como condição a examinar, “uso indevido” como ameaça possível, “acesso não autorizado” como evento e “exposição ou alteração de informação” como consequências a investigar. O exemplo não descreve incidente real.

8.2 Phishing: definição e controles

Phishing é descrito como processo fraudulento para obter informações sensíveis ao se apresentar como entidade confiável em uma comunicação eletrônica. Pode usar e-mail ou mensagem instantânea, direcionar a páginas falsas ou instalar mecanismos que capturam credenciais [39] [40].

No contexto de infraestrutura em saúde, a fonte destaca treinamento para reconhecimento de ameaças, autenticação em dois fatores, restrições à instalação de software, práticas robustas de prevenção e responsabilização dos usuários [41].

Análise conjuntamente mensagem, interface, pressão de tempo, autenticação, detecção, processo e condições de trabalho; depois relacione cada condição a uma barreira de prevenção, detecção ou resposta.

8.3 Ransomware e indisponibilidade

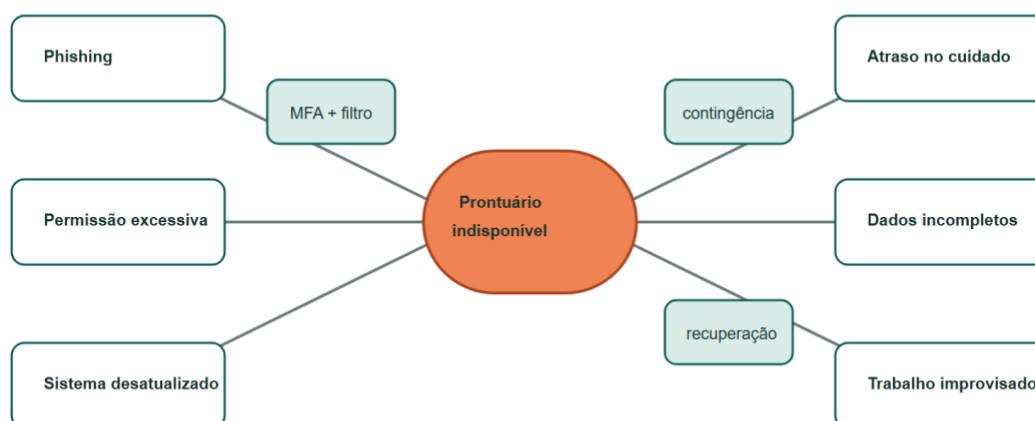
A fonte descreve ransomware como situação em que atacantes bloqueiam o acesso aos dados e exigem pagamento para liberar o acesso. Ela destaca que o dado não precisa ser removido para que a organização perca sua capacidade de utilizá-lo [42].

A consequência central para este encontro é a indisponibilidade. Mesmo quando a confidencialidade não é o primeiro efeito visível, o cuidado pode perder acesso a prontuários, interfaces, resultados e canais de comunicação. A fonte sobre EHR orienta

desenvolver procedimentos de downtime e planos de recuperação, definir papéis e reconciliar dados produzidos durante a falha [32].

8.4 Bow-tie: barreiras antes e depois do evento

Incidente: barreiras antes, durante e depois



Responsabilidade compartilhada: desenho, processo, pessoas, liderança e tecnologia.

Modelo pedagógico bow-tie para analisar um incidente

Leia o diagrama da esquerda para a direita.

- À esquerda, descreva condições e ameaças que podem levar ao evento central.
- Antes do evento, posicione barreiras de prevenção e detecção.
- Depois do evento, posicione resposta, continuidade e recuperação.
- À direita, explicita consequências assistenciais, informacionais e organizacionais.

O modelo é autoral e não representa incidente real. Sua utilidade é distribuir responsabilidade entre barreiras, evitando reduzir segurança a uma única pessoa ou a um único controle.

8.5 Controles precisam formar um conjunto

A fonte recomenda políticas uniformes, treinamento, detecção de intrusão, controles de acesso e trilhas de auditoria. Outro trecho destaca procedimentos de downtime testados e suporte contínuo como mudanças complementares à implantação de sistemas [35] [43].

Organize controles por momento:

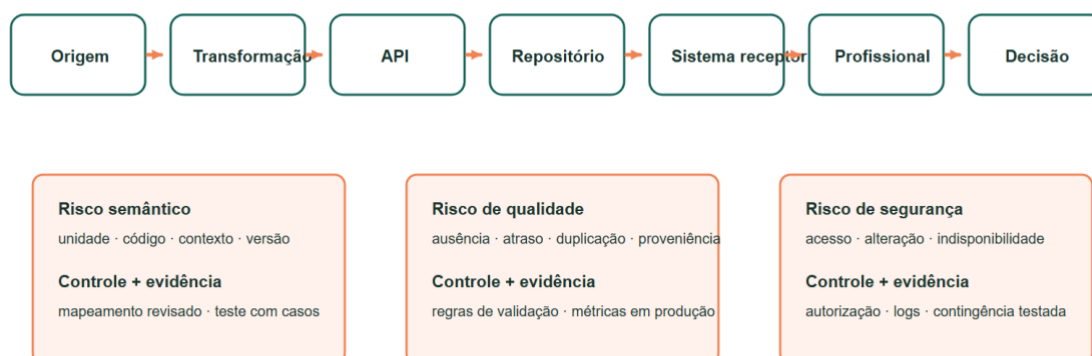
Momento	Pergunta	Exemplos apoiados ou derivados das fontes
prevenir	como reduzir a possibilidade do evento?	políticas, treinamento, controles de acesso

Momento	Pergunta	Exemplos apoiados ou derivados das fontes
detectar	como perceber comportamento ou alteração indevida?	detecção de intrusão, auditoria, revisão
responder	como conter, comunicar e coordenar?	papéis definidos e procedimentos operacionais
recuperar	como restaurar e reconciliar?	downtime, recuperação, verificação e entrada posterior

Os agrupamentos “prevenir, detectar, responder e recuperar” são uma organização pedagógica. Os exemplos foram construídos a partir dos controles e dos processos descritos nas fontes [35] [32].

8.6 Interoperabilidade amplia dependências

Cada passagem cria evidências — e novos riscos



Governança conjunta: quem detecta, decide, responde e aprende?

Percurso do dado com riscos, controles e evidências

Aplicação ao caso. Quando mais sistemas participam do percurso, erros podem ser replicados, autorizações precisam atravessar novas fronteiras, a disponibilidade de um componente pode depender de outros e a reconstrução do percurso pode ficar distribuída entre vários registros. Essa inferência se apoia na necessidade documentada de corrigir dados no sistema de origem e nos receptores, na existência de diferenças locais e na complexidade de equilibrar acesso e segurança [7] [3] [35].

O diagrama é uma síntese didática. Em cada etapa, pergunte: qual é o risco, quem responde, que controle atua e que evidência demonstra funcionamento?

8.7 Caso Celina: sistema indisponível

Retomando o caso.

Durante a internação, o prontuário fica temporariamente indisponível. A equipe acessa um PDF antigo e uma pessoa propõe compartilhar uma fotografia por canal não autorizado para acelerar o cuidado.

Divida a análise em três colunas:

Confidencialidade	Integridade	Disponibilidade
quem poderá ver a fotografia?	qual versão do PDF está sendo usada?	que informação precisa estar acessível agora?
onde a imagem permanecerá?	como decisões serão registradas?	qual canal de contingência existe?
que acesso será auditável?	como ocorrerá reconciliação posterior?	quem ativa e encerra a contingência?

Não reduza a situação a “certo” ou “errado”. Pergunte quais condições tornaram o atalho provável, quais riscos ele tenta reduzir, quais riscos desloca e que barreiras permitiriam trabalhar sem recorrer a um canal não autorizado.

8.8 Desenhar uma contingência realista

Os capítulos processados recomendam políticas e procedimentos para manutenção e falha, uso temporário de formulários e comunicações alternativas, definição de papéis, recuperação e incorporação posterior dos registros produzidos durante a indisponibilidade [32].

Roteiro de trabalho.

1. **Gatilho:** quem declara a indisponibilidade e com qual evidência?
2. **Dado mínimo:** que informação precisa continuar acessível para a decisão delimitada?
3. **Canal autorizado:** como o dado será obtido, comunicado e protegido?
4. **Registro:** onde ficam documentadas as decisões durante a falha?
5. **Responsabilidade:** quem coordena, comunica, corrige e encerra?
6. **Restauração:** como dados temporários serão reconciliados com o sistema?
7. **Teste:** que cenário demonstra que o plano funciona e que efeito adverso precisa ser monitorado?

A atividade não substitui plano institucional de continuidade. Ela treina a explicitação de dependências e responsabilidades.

9. Oficina integrada: um percurso auditável

9.1 Missão do grupo

Mapear um dado do projeto ou da prática que precise circular, preservando significado e contexto e analisando segurança, privacidade, correção e disponibilidade.

Escolha uma decisão concreta. Somente depois escolha o dado. Temas possíveis para exercício fictício: glicemia, alergia, dor, lesão por pressão, medicamentos, sinais vitais, plano de cuidados ou transição entre serviços.

Não utilize dados reais identificáveis, telas institucionais nem credenciais. O produto é um modelo de raciocínio, não uma reprodução do ambiente de trabalho.

9.2 Canvas integrado

Canvas · intercâmbio clínico seguro

DECISÃO ASSISTENCIAL · quem decide? com que consequência de erro?				
ORIGEM → DESTINO	DADOS MÍNIMOS	CONTEXTO / TEMPO	TERMINOLOGIA	RECURSOS FHIR
TRANSFORMAÇÃO / VALIDAÇÃO	PROVENIÊNCIA / LACUNAS		PERDA OU INCERTEZA SEMÂNTICA	
ATIVO / AMEAÇA	VULNERABILIDADE	INCIDENTE / EFEITO	PREVENIR / DETECTAR	RESPONDER / RECUPERAR
RISCO RESIDUAL / EFEITO ADVERSO	MÉTRICA / EVIDÊNCIA		QUESTÃO ABERTA / RESPONSÁVEL	

Canvas de interoperabilidade e segurança para a oficina

A metade superior do canvas acompanha decisão, origem, destino, dados, contexto, terminologia, transformação e incerteza. A metade inferior acompanha ativo, vulnerabilidade, ameaça, controles, risco residual e avaliação.

O campo FHIR é opcional. Preenchê-lo sem necessidade técnica não melhora o produto. Se o grupo não possui fonte oficial e versão aplicável, registre a questão em aberto.

9.3 Seis etapas em 70 minutos

Etapa	Tempo	Produto parcial
situação e decisão	10 min	origem, destino,

Etapa	Tempo	Produto parcial
		responsável e consequência de erro
dados e contexto	12 min	conjunto mínimo, ausências e proveniência
mapeamento semântico	12 min	termo local, conceito, perda ou incerteza
responsabilidade e acesso	10 min	atores, permissões e correção
ameaça, controles e contingência	16 min	evento, barreiras e continuidade
crítica sociotécnica	10 min	risco residual, efeito adverso e métrica

O facilitador deve perguntar repetidamente qual decisão está em análise. Se o grupo começa pela tecnologia, volte ao primeiro campo.

9.4 Papéis para distribuir perspectivas

Distribua funções de análise, não profissões:

- guardião da decisão clínica;
- curador de dados, contexto e proveniência;
- analista de significado e terminologia;
- analista de acesso, ameaça e continuidade;
- crítico do trabalho real e de efeitos adversos;
- relator, quando houver sexta pessoa.

Em grupos menores, combine papéis. Na apresentação, alterne a pessoa que fala para evitar que uma única perspectiva concentre o raciocínio.

9.5 Entregável

O grupo deverá produzir:

1. diagrama do percurso entre origem e destino;
2. conjunto mínimo de dados e contexto para a decisão;
3. descrição de proveniência, transformações e dados ausentes;
4. mapeamento semântico com perda, ambiguidade ou incerteza visível;
5. atores, acesso e responsabilidade por correção;
6. ameaça, controles e contingência;
7. risco residual, possível efeito adverso do controle e métrica;

8. questão técnica, normativa ou jurídica que permanece aberta.

O grupo não precisa apresentar códigos terminológicos reais. Caso escolha fazê-lo, deve registrar fonte e versão verificadas; como essas fontes oficiais não fazem parte do corpus processado, o código não poderá ser validado automaticamente por esta apostila.

9.6 Teste de qualidade antes de apresentar

Critério	Pergunta de teste
decisão	está clara, situada e ligada a uma consequência?
contexto	o receptor sabe interpretar o dado?
proveniência	origem, tempo e transformação podem ser reconstruídos?
terminologia	perda, ambiguidade e versão estão visíveis?
especificação	o aprofundamento técnico é necessário e sustentado?
segurança	controles cobrem prevenção, detecção, resposta e recuperação?
trabalho	há novo ônus, atraso, bloqueio ou atalho provável?
avaliação	a métrica demonstra algo útil para a decisão?

O checklist é formativo. Ele privilegia justificativa, rastreabilidade e reconhecimento de limites, não sofisticação técnica.

9.7 Apresentação e crítica entre pares

Cada grupo terá de cinco a sete minutos para apresentar o encadeamento:

decisão → dado → significado → intercâmbio → risco → controle → avaliação

Outro grupo atuará como debatedor e responderá:

1. o que está mais bem fundamentado;
2. que ambiguidade semântica permanece;
3. que risco foi subestimado;
4. que controle pode gerar efeito adverso;
5. que pressuposto precisa ser testado;
6. que questão exige fonte oficial adicional.

Evite críticas genéricas. Toda observação deve apontar um campo do canvas, uma relação ou uma ausência específica.

10. Retorno ao caso Celina e síntese

10.1 O caso depois do percurso

Retomando o caso.

Agora a equipe recebeu uma glicemia acompanhada de unidade e informações de origem; a alergia está associada a uma incerteza explícita; a observação de enfermagem foi incorporada ao fluxo; e existe um procedimento de contingência a ser testado.

Ainda não é suficiente para “confiar”. A equipe precisa verificar identidade, atualidade, contexto, transformações, autorização, versão, incorporação ao trabalho e resultado do uso. O desfecho não é evidência empírica; ele serve para mostrar que interoperabilidade é uma propriedade a ser verificada no percurso, não uma etiqueta aplicada ao sistema.

10.2 Síntese visual

Dado que circula precisa continuar confiável e utilizável



Padrões reduzem ambiguidades; governança, testes e trabalho real determinam o efeito.

Síntese do percurso entre interoperabilidade e segurança

Leia o diagrama de fora para dentro. Proteção, qualidade, significado e contexto precisam convergir para uma decisão. Depois leia de dentro para fora: a decisão define quais dados, significados, condições de qualidade e proteções são necessários.

10.3 Três mensagens essenciais

1. **Transportar não preserva automaticamente o significado.** Conectividade e mensagens são necessárias, mas diferenças de representação, códigos, contexto e processo permanecem [5] [4].

2. **Padronizar não elimina governança e teste.** Terminologias e estruturas ajudam a tornar dados comparáveis, mas correção, atualização, mapeamento e uso continuam exigindo responsáveis e evidências [15] [7].
3. **Proteger inclui manter o dado correto e disponível.** Confidencialidade, integridade, auditoria, acesso autorizado e continuidade precisam ser analisados em relação ao cuidado [31] [32].

10.4 Minuto de saída

Complete três frases.

- Antes eu tratava interoperabilidade como...
- Agora verificarei também...
- No meu projeto ou serviço, a próxima pergunta que preciso fazer é...

11. Glossário comentado do Encontro 3

Termo	Explicação utilizada nesta apostila
prontuário eletrônico de saúde	registro eletrônico longitudinal que reúne informações de encontros de cuidado, apoia workflow e outras funções relacionadas ao cuidado [2].
conectividade	Rótulo pedagógico: existência de caminho técnico para comunicação; isoladamente não garante comparabilidade, significado ou uso [5].
interoperabilidade semântica	troca de dados sem perda de contexto ou significado, permitindo reutilização sem esforço especial por parte do usuário [4].
dado estruturado	dado organizado em formato predefinido e frequentemente apresentado como elementos discretos [1].
qualidade do dado	Organização pedagógica: adequação examinada por presença, unicidade, validade, consistência, atualidade e uso pretendido; não é escala validada. O suporte documental inclui precisão, completude, atualização e perda de contexto [9] [11].
proveniência	Para os fins deste exercício, informações

Termo	Explicação utilizada nesta apostila
	que permitem reconstruir origem, autoria, tempo, transformação, versão e correção de um dado. A fonte sustenta os componentes de auditoria e correção, mas não apresenta definição normativa do termo [7] [14].
terminologia padronizada	vocabulário usado para representar conceitos de modo compartilhado e facilitar entendimento, comparação e intercâmbio [15].
LOINC	terminologia descrita para observações, perguntas, variáveis e avaliações [8].
SNOMED CT	terminologia associada nas fontes a diagnósticos, sintomas, achados, organismos e respostas [8].
ICNP	linguagem comum de códigos para dados de enfermagem, descrita como relevante para intercâmbio que preserve significado entre contextos [19].
mapeamento semântico	Para os fins deste exercício, relação documentada entre expressão local, conceito, código, atributos e uso receptor; deve explicitar perda ou incerteza. As fontes sustentam tradução de códigos e exemplos de mapeamento, mas não esta definição operacional [21] [22].
FHIR	padrão da HL7 voltado à Web, baseado em recursos modulares e tecnologias como XML, JSON, HTTP e OAuth [24].
recurso FHIR	unidade básica de interoperabilidade e componente modular que pode ser combinado em sistemas [25].
API RESTful	interface descrita na fonte como uso de requisições HTTP para GET, PUT, POST e DELETE dados [24].
confidencialidade	nesta apostila, propriedade examinada pela restrição do acesso a identidades autorizadas e pelas condições de compartilhamento [33].
integridade	propriedade que pode ser comprometida

Termo	Explicação utilizada nesta apostila
	por entrada incorreta, adulteração ou falha do sistema e que depende de correção, auditoria, políticas e procedimentos [10].
disponibilidade	nesta apostila, capacidade de usuários autorizados acessarem informação no momento necessário, com procedimentos para manutenção e falha [31] [32].
trilha de auditoria	mecanismo que permite acompanhar quem inseriu ou modificou um elemento e registrar data, hora e identidade [7] [14].
ransomware	forma de ataque descrita como bloqueio do acesso aos dados com exigência de pagamento para liberação [42].
downtime	período de indisponibilidade que exige procedimentos alternativos, papéis definidos, recuperação e reconciliação posterior [32].
contingência	nesta apostila, a expressão designa conjunto de gatilhos, dados mínimos, canais, registros, responsabilidades e procedimentos de restauração para manter o trabalho durante a falha; não substitui plano institucional.

12. Atividades de consolidação

Atividade 1 — Autópsia de um dado que “chegou”

Escolha um elemento fictício do caso Celina e preencha:

1. origem e destino;
2. estrutura em que foi enviado;
3. significado pretendido;
4. contexto necessário;
5. transformação realizada;
6. falha predominante;
7. segunda camada envolvida;
8. consequência para a decisão;

9. evidência necessária para considerar a falha resolvida.

Atividade 2 — Qualidade situada

Compare três situações.

Situação	Técnica	Contexto	Atualidade	Incorporação ao trabalho
A	válida	ausente	recente	incerta
B	válida	presente	antiga	presente
C	válida	presente	recente	ausente

Para cada linha, responda: qual decisão seria prejudicada, que informação falta e quem precisa agir? Não classifique uma linha como universalmente “pior”. A consequência depende do uso.

Atividade 3 — Auditoria de mapeamento

Escolha uma expressão local ambígua e produza uma ficha com:

- expressão original;
- conceito pretendido;
- atributos ausentes;
- terminologia possivelmente aplicável;
- perda possível;
- pessoa ou função responsável por esclarecer;
- maneira de representar incerteza;
- regra de revisão do mapeamento.

Atividade 4 — Sucesso técnico versus sucesso clínico

Imagine que uma API retornou sucesso ao enviar um dado. Liste uma evidência para cada pergunta:

1. a estrutura foi aceita?
2. o conceito foi interpretado como pretendido?
3. a unidade foi preservada?
4. o dado estava atual?
5. a pessoa estava corretamente identificada?
6. o dado entrou no workflow?
7. a correção poderia ser propagada?
8. o uso foi autorizado e auditável?

Atividade 5 — Bow-tie de indisponibilidade

Construa um bow-tie com o evento central “prontuário indisponível”. Inclua:

- duas condições que favorecem o evento;
- duas barreiras de prevenção;
- duas formas de detecção;
- três consequências possíveis;
- duas ações de resposta;
- duas ações de recuperação;
- uma evidência de que a contingência foi testada;
- um efeito adverso criado pelo próprio controle.

Atividade 6 — Parecer de limites

Redija um parágrafo que explique a um gestor por que a proposta ainda não pode ser apresentada como especificação da RNDS, parecer de LGPD ou guia de implementação FHIR. O texto deverá indicar:

1. o que está sustentado pelas fontes locais;
 2. o que permanece ausente;
 3. qual documento oficial precisa ser consultado;
 4. que decisão não pode ser tomada ainda.
-

13. Questões para discussão

Utilize as perguntas em seminário, estudo dirigido ou revisão individual.

1. Em que ponto do caso Celina conexão foi confundida com interoperabilidade?
2. Por que um campo reconhecido pelo receptor ainda pode permanecer semanticamente frágil?
3. O que diferencia transportar “alergia forte” de representar uma informação utilizável?
4. Qual camada de interoperabilidade costuma ficar invisível em projetos conhecidos por você?
5. Quando um dado presente pode continuar inadequado ao uso?
6. Que componentes de contexto acompanham uma medida no seu projeto?
7. Como a correção de um erro deve percorrer os sistemas receptores?
8. Que elemento de proveniência é mais difícil de reconstruir em sua prática?
9. Quando a padronização aumenta comparabilidade e quando pode reduzir nuance?

10. Por que LOINC, SNOMED CT e uma linguagem de dados de enfermagem podem ser complementares?
11. Que perda precisa permanecer explícita em um mapeamento semântico?
12. Que perguntas devem ser respondidas antes de mencionar RNDS como solução?
13. O que FHIR oferece segundo as fontes e o que ele não garante?
14. Por que uma requisição tecnicamente bem-sucedida não demonstra adequação clínica?
15. Que diferença existe entre autenticar, autorizar e auditar?
16. Como um controle de acesso pode proteger informação e simultaneamente criar atraso?
17. Que consequência assistencial decorre de falha de integridade?
18. Que consequência assistencial decorre de indisponibilidade?
19. Por que a discussão de privacidade não pode ser reduzida a uma senha?
20. Que informação legal precisa ser consultada antes de formular conclusão sobre LGPD?
21. Como ransomware transforma um problema de segurança em problema de continuidade?
22. Que barreira atua antes do evento e que barreira limita consequências depois dele?
23. Como avaliar se um plano de downtime é realmente utilizável?
24. Que risco novo sua contingência pode criar?
25. Que métrica demonstraria que o percurso melhorou a decisão pretendida?

14. Autoavaliação

Assinale sua situação ao final do encontro.

Afirmiação	Ainda não	Em construção	Consigo explicar e aplicar
Distingo conectividade e, transporte, estrutura, significado e incorporação ao trabalho.	☐	☐	☐
Explico interoperabilidade	☐	☐	☐

Afirmação	Ainda não	Em construção	Consigo explicar e aplicar
semântica sem reduzi-la a troca de arquivos.			
Analiso qualidade em relação a uma decisão delimitada.	☐	☐	☐
Reconstruo origem, transformação e correção de um dado.	☐	☐	☐
Diferencio os papéis documentados para LOINC, SNOMED CT e ICNP.	☐	☐	☐
Reconheço perda e incerteza em um mapeamento.	☐	☐	☐
Explico recursos e API FHIR sem prometer interoperabilidade automática.	☐	☐	☐
Analiso confidencialidade,	☐	☐	☐

Afirmação	Ainda não	Em construção	Consigo explicar e aplicar
integridade e disponibilidade de no cuidado.			
Proponho controles antes e depois de uma indisponibilidade.	☐	☐	☐
Desenho uma contingência com reconciliação posterior.	☐	☐	☐
Identifico quando RNDS, LGPD ou FHIR exigem fonte oficial adicional.	☐	☐	☐
Comunico limites e questões abertas sem escondê-los.	☐	☐	☐

Pausa de síntese. Escolha uma afirmação marcada “em construção” e escreva que evidência permitiria movê-la para “consigo explicar e aplicar”.

Apêndice — Rastreabilidade

Matriz de rastreabilidade

Objetivo de aprendizagem	Tópico	Atividade	Fonte	Página	Trecho
Explicar por que conexão não garante significado	conectividade e interoperabilidade semântica	diagnóstico das quatro camadas	1- Informatics-for-Nurses__XIV-The-Electronic-Health-Record.pdf; 4-Health-Informatics__XXIV-Safety-and-Quality-Initiatives.pdf	13; 17	1- informatics-for-nurses-xiv-the-electronic-health-record__p0013__c002; 4-health-informatics-xxiv-safety-and-quality-initiatives__p0017__c001
Analisar significado, contexto e qualidade	adequação ao uso e representação	autópsia de um dado; qualidade situada	2- Biomedical-Informatics__XIV-Electronic-Health-Records.pdf; 1- Informatics-for-Nurses__XIV-The-Electronic-Health-Record.pdf	8–9; 15	2- biomedical-informatics-xiv-electronic-health-records__p0008__c001; 2- biomedical-informatics-xiv-electronic-health-records__p0009__c001; 1- informatics-for-nurses-xiv-the-

Objetivo de aprendizagem	Tópico	Atividade	Fonte	Página	Trecho
					electronic-health-record__p0015__c001
Reconstruir proveniência e correção	auditoria, autoria, tempo e propagação	ficha de proveniência	1- Informatics-for-Nurses__XIV-The-Electronic-Health-Record.pdf; 6- Extra__Provenance-FHIR-v4-3-0.pdf; 6- Extra__PROV-O-The-PROV-Ontology.pdf	15; 17; 1; 1	1- informatics-for-nurses-xiv-the-electronic-health-record__p0015__c002; 1- informatics-for-nurses-xiv-the-electronic-health-record__p0017__c001; 6-extra-provenance-fhir-v4-3-0__p0001__c001; 6-extra-prov-o-the-prov-ontology__p0001__c001
Reconhecer o papel de terminologias	LOINC, SNOMED CT e ICNP	auditoria de mapeamento	2- Biomedical-Informatics__XIV-The-Electronic-Health-Records.pdf; 1- Informatics-for-	9; 12	2- biomedical-informatics-xiv-electronic-health-records__p0009__c001; 1- informatics-

Objetivo de aprendizagem	Tópico	Atividade	Fonte	Página	Trecho
			Nurses__I- Informatics- in-the- Healthcare- Professions. pdf		for-nurses-i- informatics- in-the- healthcare- professions __p0012__c 001
Reconhecer limites do mapeamento	tradução, equivalência e incerteza	termo “alergia forte”	2- Biomedical- Informatics_ _XIV- Electronic- Health- Records.pdf	10; 18	2- biomedical- informatics- xiv- electronic- health- records__p0 010__c001; 2- biomedical- informatics- xiv- electronic- health- records__p0 018__c001
Explicar FHIR sem automatismo	recursos, tecnologias Web, perfis, extensões e API RESTful	sucesso técnico versus sucesso clínico	2- Biomedical- Informatics_ _XXIV- Clinical- Decision- Support- Systems.pdf ; 6- Extra__Profil ing-FHIR-v4- 0-1.pdf; 6- Extra__Exte nsibility- FHIR-v4-0-	32; 2; 1	2- biomedical- informatics- xxiv-clinical- decision- support- systems__p 0032__c001 ; 2- biomedical- informatics- xxiv-clinical- decision- support- systems__p 0032__c002

Objetivo de aprendizagem	Tópico	Atividade	Fonte	Página	Trecho
			1.pdf		; 6-extra-profiling-fhir-v4-0-1__p0002__c001; 6-extra-extensibility-fhir-v4-0-1__p0001__c001; 6-extra-extensibility-fhir-v4-0-1__p0001__c002
Analisar confidencialidade, integridade e disponibilidade	segurança como propriedade do cuidado	matriz CIA do caso Celina	1- Informatics-for-Nurses__XIV-The-Electronic-Health-Record.pdf	6; 15–16	1- informatics-for-nurses-xiv-the-electronic-health-record__p0006__c001; 1- informatics-for-nurses-xiv-the-electronic-health-record__p0015__c001; 1- informatics-for-nurses-xiv-the-electronic-health-record__p0016__c001

Objetivo de aprendizagem	Tópico	Atividade	Fonte	Página	Trecho
Relacionar ameaça, controle e consequência	ransomware e barreiras	bow-tie de indisponibilidade	2-Biomedical-Informatics_XVI-Management-of-Information-in-Health-Care-Organizations.pdf	16	2-biomedical-informatics-xvi-management-of-information-in-health-ca-113b5c732f50__p0016__c001; 2-biomedical-informatics-xvi-management-of-information-in-health-ca-113b5c732f50__p0016__c002
Propor contingência	downtime, recuperação e reconciliação	roteiro de contingência	1-Informatics-for-Nurses_XIV-The-Electronic-Health-Record.pdf	16	1-informatics-for-nurses-xiv-the-electronic-health-record__p0016__c001
Comunicar raciocínio auditável	percurso integrado	canvas, apresentação e crítica entre pares	síntese das fontes acima	—	—

Fontes citadas

Os números apresentados ao longo do texto remetem às referências documentais abaixo. Cada entrada preserva o arquivo, a página e o identificador do trecho utilizado.

1. [Fonte: 1-Informatics-for-Nurses__XIV-The-Electronic-Health-Record.pdf, p. 03, trecho: 1-informatics-for-nurses-xiv-the-electronic-health-record__p0003__c001]
2. [Fonte: 1-Informatics-for-Nurses__XIV-The-Electronic-Health-Record.pdf, p. 04, trecho: 1-informatics-for-nurses-xiv-the-electronic-health-record__p0004__c001]
3. [Fonte: 2-Biomedical-Informatics__XIV-Electronic-Health-Records.pdf, p. 08, trecho: 2-biomedical-informatics-xiv-electronic-health-records__p0008__c001]
4. [Fonte: 4-Health-Informatics__XXIV-Safety-and-Quality-Initiatives.pdf, p. 17, trecho: 4-health-informatics-xxiv-safety-and-quality-initiatives__p0017__c001]
5. [Fonte: 1-Informatics-for-Nurses__XIV-The-Electronic-Health-Record.pdf, p. 13, trecho: 1-informatics-for-nurses-xiv-the-electronic-health-record__p0013__c002]
6. [Fonte: 1-Informatics-for-Nurses__XIV-The-Electronic-Health-Record.pdf, p. 11, trecho: 1-informatics-for-nurses-xiv-the-electronic-health-record__p0011__c002]
7. [Fonte: 1-Informatics-for-Nurses__XIV-The-Electronic-Health-Record.pdf, p. 15, trecho: 1-informatics-for-nurses-xiv-the-electronic-health-record__p0015__c002]
8. [Fonte: 2-Biomedical-Informatics__XIV-Electronic-Health-Records.pdf, p. 09, trecho: 2-biomedical-informatics-xiv-electronic-health-records__p0009__c001]
9. [Fonte: 1-Informatics-for-Nurses__XIV-The-Electronic-Health-Record.pdf, p. 08, trecho: 1-informatics-for-nurses-xiv-the-electronic-health-record__p0008__c001]
10. [Fonte: 1-Informatics-for-Nurses__XIV-The-Electronic-Health-Record.pdf, p. 15, trecho: 1-informatics-for-nurses-xiv-the-electronic-health-record__p0015__c001]
11. [Fonte: 2-Biomedical-Informatics__XIV-Electronic-Health-Records.pdf, p. 12, trecho: 2-biomedical-informatics-xiv-electronic-health-records__p0012__c002]
12. [Fonte: 6-Extra__Provenance-FHIR-v4-3-0.pdf, p. 01, trecho: 6-extra-provenance-fhir-v4-3-0__p0001__c001]
13. [Fonte: 6-Extra__PROV-O-The-PROV-Ontology.pdf, p. 01, trecho: 6-extra-prov-o-the-prov-ontology__p0001__c001]
14. [Fonte: 1-Informatics-for-Nurses__XIV-The-Electronic-Health-Record.pdf, p. 17, trecho: 1-informatics-for-nurses-xiv-the-electronic-health-record__p0017__c001]
15. [Fonte: 1-Informatics-for-Nurses__XIV-The-Electronic-Health-Record.pdf, p. 14, trecho: 1-informatics-for-nurses-xiv-the-electronic-health-record__p0014__c001]

16. [Fonte: 4-Health-Informatics__VII-The-Electronic-Health-Record-and-Precision-Care.pdf, p. 22, trecho: 4-health-informatics-vii-the-electronic-health-record-and-precision-care__p0022__c001]
17. [Fonte: 6-Extra__LOINC-Release-Notes-KB-LOINC.pdf, p. 01, trecho: 6-extra-loinc-release-notes-kb-loinc__p0001__c001]
18. [Fonte: 1-Informatics-for-Nurses__XIV-The-Electronic-Health-Record.pdf, p. 05, trecho: 1-informatics-for-nurses-xiv-the-electronic-health-record__p0005__c002]
19. [Fonte: 1-Informatics-for-Nurses__I-Informatics-in-the-Healthcare-Professions.pdf, p. 12, trecho: 1-informatics-for-nurses-i-informatics-in-the-healthcare-professions__p0012__c001]
20. [Fonte: 1-Informatics-for-Nurses__XV-The-Role-of-Standardized-Terminology-and-Languages-in-Informatics.pdf, p. 11, trecho: 1-informatics-for-nurses-xv-the-role-of-standardized-terminology-an-36a85df90f8a__p0011__c001]
21. [Fonte: 2-Biomedical-Informatics__XIV-Electronic-Health-Records.pdf, p. 10, trecho: 2-biomedical-informatics-xiv-electronic-health-records__p0010__c001]
22. [Fonte: 2-Biomedical-Informatics__XIV-Electronic-Health-Records.pdf, p. 18, trecho: 2-biomedical-informatics-xiv-electronic-health-records__p0018__c001]
23. [Fonte: 6-Extra__Objetivo-RNDS.pdf, p. 01, trecho: 6-extra-objetivo-rnds__p0001__c001]
24. [Fonte: 2-Biomedical-Informatics__XXIV-Clinical-Decision-Support-Systems.pdf, p. 32, trecho: 2-biomedical-informatics-xxiv-clinical-decision-support-systems__p0032__c001]
25. [Fonte: 2-Biomedical-Informatics__XXIV-Clinical-Decision-Support-Systems.pdf, p. 32, trecho: 2-biomedical-informatics-xxiv-clinical-decision-support-systems__p0032__c002]
26. [Fonte: 2-Biomedical-Informatics__XIV-Electronic-Health-Records.pdf, p. 11, trecho: 2-biomedical-informatics-xiv-electronic-health-records__p0011__c001]
27. [Fonte: 2-Biomedical-Informatics__XIV-Electronic-Health-Records.pdf, p. 15, trecho: 2-biomedical-informatics-xiv-electronic-health-records__p0015__c001]
28. [Fonte: 6-Extra__Profiling-FHIR-v4-0-1.pdf, p. 02, trecho: 6-extra-profiling-fhir-v4-0-1__p0002__c001]
29. [Fonte: 6-Extra__Extensibility-FHIR-v4-0-1.pdf, p. 01, trecho: 6-extra-extensibility-fhir-v4-0-1__p0001__c001]
30. [Fonte: 6-Extra__Extensibility-FHIR-v4-0-1.pdf, p. 01, trecho: 6-extra-extensibility-fhir-v4-0-1__p0001__c002]
31. [Fonte: 1-Informatics-for-Nurses__XIV-The-Electronic-Health-Record.pdf, p. 06, trecho: 1-informatics-for-nurses-xiv-the-electronic-health-record__p0006__c001]

32. [Fonte: 1-Informatics-for-Nurses__XIV-The-Electronic-Health-Record.pdf, p. 16, trecho: 1-informatics-for-nurses-xiv-the-electronic-health-record__p0016__c001]
33. [Fonte: 1-Informatics-for-Nurses__XIV-The-Electronic-Health-Record.pdf, p. 14, trecho: 1-informatics-for-nurses-xiv-the-electronic-health-record__p0014__c002]
34. [Fonte: 1-Informatics-for-Nurses__XIV-The-Electronic-Health-Record.pdf, p. 16, trecho: 1-informatics-for-nurses-xiv-the-electronic-health-record__p0016__c002]
35. [Fonte: 2-Biomedical-Informatics__XVI-Management-of-Information-in-Health-Care-Organizations.pdf, p. 16, trecho: 2-biomedical-informatics-xvi-management-of-information-in-health-ca-113b5c732f50__p0016__c002]
36. [Fonte: 6-Extra__L13709compilado.pdf, p. 02, trecho: 6-extra-l13709compilado__p0002__c001]
37. [Fonte: 6-Extra__L13709compilado.pdf, p. 03, trecho: 6-extra-l13709compilado__p0003__c002]
38. [Fonte: 6-Extra__L13709compilado.pdf, p. 04, trecho: 6-extra-l13709compilado__p0004__c001]
39. [Fonte: 1-Informatics-for-Nurses__XII-Information-Security-and-Confidentiality.pdf, p. 7, trecho: 1-informatics-for-nurses-xii-information-security-and-confidentiality__p0007__c001]
40. [Fonte: 1-Informatics-for-Nurses__XII-Information-Security-and-Confidentiality.pdf, p. 7, trecho: 1-informatics-for-nurses-xii-information-security-and-confidentiality__p0007__c002]
41. [Fonte: 4-Health-Informatics__VI-Technical-Infrastructure.pdf, p. 14, trecho: 4-health-informatics-vi-technical-infrastructure__p0014__c002]
42. [Fonte: 2-Biomedical-Informatics__XVI-Management-of-Information-in-Health-Care-Organizations.pdf, p. 16, trecho: 2-biomedical-informatics-xvi-management-of-information-in-health-ca-113b5c732f50__p0016__c001]
43. [Fonte: 2-Biomedical-Informatics__XVI-Management-of-Information-in-Health-Care-Organizations.pdf, p. 15, trecho: 2-biomedical-informatics-xvi-management-of-information-in-health-ca-113b5c732f50__p0015__c002]