CORVITA / AXIS · USO INTERNO

Manual de orientação do *prontuário eletrônico*

Contrato de entendimento para os desenvolvedores sênior que construirão o MVP cardiovascular. Escrito para ser lido por gente, aplicado por engenharia e defendido perante a lei.

TESE CENTRAL

AXIS = prontuário sério + jornada multiprofissional no tempo + paciente informado. O sistema só vai a produção quando as três partes funcionarem juntas e houver evidência de segurança.

SUMÁRIO

Índice navegável do *manual*

Clique em qualquer seção para ir direto ao slide. No PDF, os itens também são links internos.

03 Como usar este manual

04 1 · O que é o AXIS em essência

07 2 · O que é prontuário, de verdade

10 3 · Arquitetura, jornada e portões clínicos

13 4 · Papéis profissionais e responsabilidade

14 5 · Obrigações jurídicas em software

17 6 · LGPD, governança e incidentes

19 7 · Segurança e continuidade

22 8 · Modelo de dados e FHIR

26 9 · Terminologias e retificação

29 10 · UX clínica

30 11 · Aceite, testes e Definition of Done

33 12 · Backlog por gates G0–G6

35 13 · Go-live e decisões da reunião

37 Apêndice A · Checklist técnico por domínio

38 Apêndice B · Fontes oficiais e técnicas

39 Encerramento

ANTES DE COMEÇAR

Como usar este manual

Este documento é a referência única para descoberta, arquitetura, implementação, QA, validação clínica e go-live. Ele não substitui parecer jurídico, certificação, avaliação de segurança nem as regras internas da clínica.

LEITURA	PARA QUE SERVE
Seções 1–4	Alinhar produto, linguagem clínica e limites de escopo.
Seções 5–7	Transformar obrigações jurídicas e de privacidade em requisitos.
Seções 8–10	Orientar arquitetura, dados, interoperabilidade e interface.
Seções 11–13	Abrir backlog, escrever testes e bloquear o go-live sem evidência.
Apêndices	Copiar modelos, payloads, matriz de papéis e fontes oficiais.

REGRA DE INTERPRETAÇÃO

MUST = obrigatório no escopo indicado. SHOULD = recomendável, com justificativa escrita se não implementado. MUST NOT = proibido. Requisito sem teste e evidência não está concluído.

SEÇÃO 1

O que é o AXIS *em essência*

O AXIS não é “um sistema de cadastro com evolução”. É a fonte oficial da verdade clínica da CorVita e, ao mesmo tempo, o mecanismo que garante que a jornada cardiovascular combinada aconteça no tempo.

ELEMENTO	O QUE PRECISA EXISTIR	FALHA SE…
Prontuário sério	histórico longitudinal, autoria, integridade, sigilo, disponibilidade, exportação	um evento some, é sobrescrito ou não tem autor
Pathway cardio	pacote, marcos, checklists, metas, multiprofissional, dossiê e KPI	o D14 pode ser “concluído” sem checklist
Paciente informado	acesso, linguagem clara, metas, próximos passos e portabilidade	a informação permanece opaca e médico-cêntrica

NA PRÁTICA Se um dos três pilares ficar para depois, o produto vira outro sistema. Nenhum deles é fase 2.

SEÇÃO 1.1

Invariantes de produto

- Todo ato clínico relevante é um evento no tempo, vinculado a paciente, autor, papel, modalidade e contexto.
- Dado clínico anterior não é silenciosamente reescrito: correção ocorre por adendo ou nova versão com vínculo.
- Enfermagem, médico, nutrição e fisioterapia registram no mesmo prontuário, dentro do próprio escopo profissional.
- Atendimento avulso usa o Core; pacote exige marcos. Um não contamina a regra do outro.
- A interface prioriza segurança e continuidade — não quantidade de campos nem estética isolada.
- Acesso do paciente não equivale a expor bastidores administrativos ou dados de terceiros.
- IA, score ou automação nunca assume diagnóstico autônomo sem avaliação médica, jurídica e regulatória.

NA PRÁTICA Estas sete frases são o teste de sanidade de qualquer PR. Se a mudança quebra uma delas, ela não entra.

SEÇÃO 1.2

O que o AXIS não é

NÃO É	DECISÃO PRÁTICA
App de wellness	Não usar linguagem de promessa, cura ou score mágico.
Motor diagnóstico autônomo	Qualquer apoio decisório exige intended use, supervisão humana e análise SaMD.
Cópia do prontuário antigo	Preservar as necessidades legais, mas redesenhar jornada e prioridade de informação.
Marketplace de especialidades no MVP	Nenhum pathway extra antes da validação cardiovascular.
Repositório de PDFs	Dados críticos precisam ser estruturados; anexos complementam, não substituem o registro.

SEÇÃO 2

O que é prontuário — *definição correta*

DEFINIÇÃO OPERACIONAL

Registro oficial, longitudinal, íntegro, disponível e auditável das informações e atos de cuidado de uma pessoa, produzido por profissionais autorizados e mantido sob custódia e responsabilidade da clínica e dos profissionais.

A frase interna “o registro é do paciente” vale como princípio de produto, não como simplificação jurídica. O paciente é titular dos dados e tem direitos previstos na LGPD; a clínica mantém deveres de custódia, sigilo, integridade, disponibilidade e documentação. O AXIS precisa sustentar os dois lados.

NA PRÁTICA Traduzindo: dar acesso ao paciente e proteger o documento clínico não são objetivos concorrentes — são requisitos simultâneos.

SEÇÃO 2.1

Propriedades esperadas e sua *implicação técnica*

PROPRIEDADE	IMPLICAÇÃO TÉCNICA
Longitudinalidade	Encounter e Observation têm effective_at; a timeline ordena o ocorrido, não apenas o updated_at.
Autoria	author_user_id, professional_role, número de registro quando aplicável, created_at e assinatura/fechamento.
Integridade	registro finalizado é imutável; adendo referencia a versão anterior; hash/assinatura conforme política.
Confidencialidade	autorização no servidor, mínimo privilégio, segregação por organização e trilha de acesso.
Disponibilidade	backup, restauração testada, contingência e exportação legível.
Completude	obrigatórios definidos por tipo de encounter, sem bloquear resposta a urgência.
Legibilidade	unidades, códigos, datas, autoria e narrativa compreensíveis por profissional e por paciente.

SEÇÃO 2.2

Estado do documento clínico

ESTADO	PODE EDITAR?	REGRA
draft	Sim, pelo autor ou equipe autorizada	rascunho não pode parecer registro final
final	Não diretamente	qualquer correção gera addendum ou retificação
entered-in-error	Não apaga	motivo obrigatório, autorização restrita e trilha preservada
amended	Nova versão vinculada	exibir o atual sem esconder o histórico

NA PRÁTICA Não existe DELETE em fato clínico. O que existe é uma nova versão que aponta para a anterior.

SEÇÃO 3.1

Core, pathway e *separação arquitetural*

CAMADA	RESPONSABILIDADE	NÃO DEVE CONHECER
Core	paciente, segurança, agenda, encounter, nota, anexo, timeline, papéis, auditoria, exportação	regras específicas de D14 ou cardiovascular
Pathway cardio	pacote, marcos D0–D90, checklists, metas, dossiê, KPI	implementação interna de autenticação, storage ou auditoria
Portal / app	visão do titular, metas, dossiê, próximos passos, pedidos de acesso e exportação	anotações administrativas e dados de terceiros sem base ou necessidade

GATE TRANSVERSAL

Nenhuma automação substitui a autoria, a revisão e a decisão humana exigidas pelo contexto clínico.

SEÇÃO 3.2

Jornada do MVP *cardiovascular*

MARCO	PROFISSIONAL / MODALIDADE	ENTREGA QUE FECHA O MARCO
D0	Enfermagem + médico, presencial	cadastro seguro, vitais, ECG/anexo, avaliação, prioridade, dossiê inicial
D14	Enfermagem, tele	identidade/privacidade, red flags, prioridade, PA, medicação, classificação e uma ação
D21	Enfermagem, tele	D14 + tendência de adesão + preparo de nutri/fisio e D30
até D30	Nutrição + fisioterapia	encounters próprios, metas e plano no escopo profissional
D30	Enfermagem + médico, presencial	novas observações, reconciliação, trajetória e ciência dos protocolos multi
D90	Equipe conforme plano	resultados, encerramento ou renovação e dossiê atualizado

INVARIANTE DE JORNADA

Um marco pode estar pending, completed, incomplete, late, no-show ou escalated. completed só é possível quando as validações obrigatórias daquela versão do protocolo foram satisfeitas.

SEÇÃO 3.3

Regra hard, alerta soft e *portão clínico*

TIPO	EXEMPLO	COMPORTAMENTO
Hard validation	PAD ≥ PAS; autor ausente; D14 sem classificação	bloqueia a finalização, mas permite salvar draft
Soft alert	PAS muito elevada; SpO_2 baixa; adesão 1–2	salva, destaca risco e exige ação ou escalonamento conforme protocolo
Clinical gate	red flag ativa	não transforma software em diagnóstico; conduz ao fluxo institucional

NA PRÁTICA O sistema pode impedir um dado impossível. Ele não pode decidir clínica no lugar do profissional.

SEÇÃO 4

Papéis profissionais e *responsabilidade*

RBAC é o ponto de partida, não a conclusão. A autorização considera organização, papel profissional, relação assistencial, estado do encounter, finalidade e contexto. Esconder botão na interface não é controle de acesso.

AÇÃO	ENFERMAGEM	MÉDICO	NUTRI/FISIO	ADMIN	PACIENTE
Ver ficha de segurança	MUST	MUST	MUST conforme cuidado	SHOULD limitado	MUST visão própria
Registrar encounter próprio	MUST	MUST	MUST	MUST NOT	MUST NOT
Editar nota final de outro	MUST NOT	MUST NOT	MUST NOT	MUST NOT	MUST NOT
Prescrever / ajustar fármaco	MUST NOT	MUST	MUST NOT	MUST NOT	MUST NOT
Retificar nota própria	MUST com trilha	MUST com trilha	MUST com trilha	MUST NOT	MUST NOT
Gerir usuários e papéis	MUST NOT	SHOULD NOT	MUST NOT	MUST	MUST NOT
Exportar prontuário	SHOULD via fluxo	SHOULD via fluxo	SHOULD via fluxo	MUST conforme política	MUST via solicitação

NA PRÁTICA Break-glass: acesso emergencial excepcional exige motivo, expira, gera alerta e auditoria reforçada. Nunca vira atalho permanente para permissões mal desenhadas.

SEÇÃO 5

Obrigações jurídicas *traduzidas em software*

A matriz abaixo não é parecer jurídico. É o conjunto mínimo de perguntas que jurídico, liderança clínica e engenharia precisam fechar antes do go-live.

FONTE	CONSEQUÊNCIA PRÁTICA PARA O AXIS	EVIDÊNCIA ESPERADA
CFM 1.638/2002	prontuário como documento único, com informações e sinais/imagens; continuidade e comunicação	modelo de prontuário e política institucional
CFM 1.821/2007 + SBIS	segurança e validade do prontuário eletrônico; requisitos mais rigorosos para eliminar o papel	gap assessment SBIS e decisão formal sobre paperless
Lei 13.787/2018	guarda com integridade, autenticidade e confidencialidade; mínimo de 20 anos após o último registro	política de retenção, exportação e descarte
LGPD (Lei 13.709/2018)	dados de saúde são sensíveis: finalidade, necessidade, segurança, direitos do titular e prestação de contas	ROPA, bases legais, DPA, RIPD quando aplicável e canal do titular
CFM 2.314/2022	telemedicina registrada em prontuário, preservando integridade, veracidade, privacidade e sigilo	tipo/modalidade, identidade, termos e registro do atendimento

Enfermagem, incidentes e *software como dispositivo*

FONTE	CONSEQUÊNCIA PRÁTICA PARA O AXIS	EVIDÊNCIA ESPERADA
Cofen 696/2022 (alterada)	telenfermagem no SUS, na saúde suplementar e no privado	fluxo D14/D21 revisado pela enfermagem e pelo RT
Cofen 754/2024	uso de prontuário eletrônico e plataformas digitais pela enfermagem	registro profissional e controles compatíveis
ANPD Res. 15/2024	incidente com risco ou dano relevante pode exigir comunicação em 3 dias úteis	runbook, relógio do incidente, registro de decisão e contatos
ANPD Res. 19/2024	transferência internacional exige mecanismo adequado e cláusulas aplicáveis	mapa de regiões, subprocessadores e contratos
Anvisa RDC 657/2022	software com intended use médico pode ser SaMD	avaliação regulatória antes de qualquer claim ou decisão autônoma

SEÇÃO 5.1

Correções importantes ao *material-base*

- Retenção: piso de referência de 20 anos após o último registro — “pode eliminar” não é “deve eliminar”. A decisão final depende da política e das normas aplicáveis.
- Consentimento não é base legal universal para tratamento assistencial; se usado, precisa ser demonstrável e revogável nos termos da lei.
- Assinatura: autenticação, fechamento, assinatura eletrônica e requisitos para paperless são arquitetura e política — não se adicionam no final.
- Certificação SBIS: usar os requisitos como baseline desde o início e decidir formalmente se e quando buscar certificação; não declarar conformidade sem avaliação.
- Paciente titular: direito de acesso não autoriza divulgar dados de terceiros, informações administrativas sem finalidade ou material sem tratamento adequado.

NA PRÁTICA Estas cinco correções são as que mais geram retrabalho quando descobertas tarde. Feche-as no gate G0.

SEÇÃO 6.1

LGPD: mapa mínimo *de tratamento*

FINALIDADE	DADOS	BASE / JUSTIFICATIVA	RETENÇÃO	ACESSO
assistência e continuidade	identificação, história, exames, notas	definir com jurídico; frequentemente tutela da saúde	política do prontuário	equipe assistencial autorizada
agenda e comunicação	contatos, preferências, horários	execução do serviço ou legítima finalidade conforme análise	mínimo necessário	atendimento e paciente
faturamento	identificação, serviço, valores	obrigação legal ou execução contratual	fiscal / contratual	financeiro restrito
analytics de produto	eventos de uso e desempenho	minimização; preferir agregado ou pseudonimizado	prazo curto e definido	produto e engenharia autorizados
pesquisa	dataset definido	base específica, ética e governança próprias	por protocolo	time aprovado

NA PRÁTICA Cada tabela nova no banco deve caber em uma linha deste mapa. Se não couber, falta decisão — não falta código.

SEÇÃO 6.2 E 6.3

Governança, contratos e *incidentes*

DOCUMENTO / CONTROLE	MUST CONTER
DPA / contrato de tratamento	objeto, instruções, sigilo, segurança, suboperadores, incidentes, devolução/eliminação, auditoria
ROPA / inventário	finalidade, categorias, titulares, sistemas, compartilhamentos, base, retenção e controles
Aviso de privacidade	linguagem clara, controlador, finalidades, direitos, canal e compartilhamentos relevantes
RIPD quando aplicável	necessidade, proporcionalidade, riscos, controles, risco residual e responsáveis
Transferência internacional	regiões, exportador e importador, mecanismo da Res. 19/2024 e cláusulas

- 1. Detectar e classificar: confidencialidade, integridade, disponibilidade, titulares e dados afetados.
- 2. Conter e preservar evidência — não apagar logs nem reiniciar indiscriminadamente.
- 3. Acionar controlador, jurídico/DPO e liderança clínica; registrar o horário da ciência.
- 4. Avaliar risco relevante e o dever de comunicar ANPD e titulares no prazo aplicável.
- 5. Corrigir, validar restauração, documentar causa raiz e ações preventivas.

SEÇÃO 7.1

Segurança: *requisitos que bloqueiam*

ID	NÍVEL	REQUISITO
SEC-01	MUST	Autorização no servidor para toda leitura e escrita de dado clínico.
SEC-02	MUST	Isolamento por organization_id/tenant testado contra IDOR e consultas sem escopo.
SEC-03	MUST	MFA para administradores e acesso privilegiado; expandir conforme risco.
SEC-04	MUST	TLS em trânsito e criptografia em repouso com gestão de chaves.
SEC-05	MUST	Segredos fora do código e dos logs; rotação e menor privilégio.
SEC-06	MUST	Audit trail de leitura, criação, fechamento, retificação, exportação e mudança de permissão.
SEC-07	MUST NOT	Registrar conteúdo clínico, tokens, senhas ou CPF completo em logs de aplicação.
SEC-08	MUST	Timeout de sessão, revogação e proteção contra sessão roubada.

SEÇÃO 7.1 E 7.2

Anexos, backup e *continuidade*

ID	NÍVEL	REQUISITO
SEC-09	MUST	Varredura de anexos, allowlist de tipo, limite de tamanho e storage privado.
SEC-10	MUST	Backup automatizado, separado e criptografado; restauração testada e documentada.
SEC-11	MUST	Monitoramento de erros, disponibilidade, ações privilegiadas e anomalias de acesso.
SEC-12	MUST	SAST, dependency scan, secret scan e revisão manual de autorização.
SEC-13	SHOULD	Pentest antes do go-live ou imediatamente antes da escala externa.
SEC-14	MUST	Ambientes separados; staging sem cópia bruta de pacientes.
SEC-15	MUST	Plano de vulnerabilidade e atualização com SLA por severidade.

SEÇÃO 7.2

Continuidade: *as quatro perguntas*

RPO

quanto dado a clínica aceita perder — para prontuário, meta explicitamente baixa

RTO

tempo máximo para restabelecer a operação

Contingência

como registrar durante indisponibilidade e reconciliar sem duplicar

Restore drill

quem executa, com que frequência, evidência e critério de sucesso

NA PRÁTICA Backup sem restauração testada é esperança, não continuidade. O drill precisa de data, responsável e evidência.

SEÇÃO 8.1

Arquitetura: *entidades mínimas*

DOMÍNIO	ENTIDADES
Identidade	Organization, User, Professional, Patient, RelatedPerson
Segurança clínica	AllergyIntolerance, Condition, MedicationStatement / MedicationRequest, Flag
Tempo clínico	Appointment, Encounter, Observation, ClinicalNote / Composition, DocumentReference
Pathway	CarePackage / EpisodeOfCare, Milestone, QuestionnaireResponse, Goal, CarePlan, Task
Governança	Consent / LegalBasisRecord, Provenance, AuditEvent, ExportRequest, AccessGrant

EVENT SOURCING LEVE

Não é preciso adotar event sourcing completo. O requisito é mais simples e inegociável: fatos clínicos finalizados não são atualizados de modo destrutivo. Tabelas relacionais convencionais bastam, desde que histórico, autoria e retificações fiquem preservados e consultáveis.

SEÇÃO 8.2

Campos transversais *obrigatórios*

CAMPO	REGRA
id	UUID ou identificador não previsível e estável
organization_id	presente e obrigatório em todo agregado multi-tenant
patient_id	vínculo consistente; fusão de duplicados por fluxo auditado
encounter_id	contexto do ato clínico quando aplicável
status	draft / final / amended / entered-in-error conforme o tipo

Tempo, autoria e *histórico*

CAMPO	REGRA
effective_at	quando o fato ocorreu ou foi medido
recorded_at	quando o fato entrou no sistema
author_id + role	quem registrou e sob qual papel profissional
version / supersedes_id	histórico e vínculo de retificação
created_at / updated_at	metadados técnicos; não substituem effective_at

NA PRÁTICA effective_at e recorded_at são coisas diferentes e ambos são obrigatórios. Confundi-los inutiliza a timeline.

SEÇÃO 8.3

FHIR como contrato de *interoperabilidade*

O AXIS não precisa espelhar FHIR literalmente no banco. Precisa, porém, evitar um modelo incompatível — com uma camada de mapeamento para exportação e futuras integrações, como a RNDS.

AXIS	FHIR R4 APROXIMADO	OBSERVAÇÃO
Paciente	Patient	identificadores, contatos, sexo ao nascer e comunicação
Consulta / tele	Encounter	atividade ocorrida; Appointment é o planejado
Vitais / IMC	Observation	effectiveDateTime, UCUM e LOINC quando possível
Alergia	AllergyIntolerance	substância, reação, criticidade e status
Anexo / ECG	DocumentReference	metadados; binário protegido em storage
Checklist	QuestionnaireResponse	versão do questionário preservada
Autoria	Provenance	origem, agente e atividade
Auditoria	AuditEvent	acesso e ação de segurança

SEÇÃO 9.2 E 9.3

Dados padronizados: *LOINC e UCUM*

DADO	LOINC	UCUM
Painel de PA	85354-9	—
PAS	8480-6	mm[Hg]
PAD	8462-4	mm[Hg]
Frequência cardíaca	8867-4	/min
Temperatura corporal	8310-5	Cel
Peso corporal	29463-7	kg
Altura	8302-2	cm
IMC	39156-5	kg/m2

NA PRÁTICA Códigos baseados no perfil HL7 FHIR R4 Vital Signs/LOINC. Confirmar terminologia e perfis nacionais no momento da integração.

SEÇÃO 9.3

Payload sintético de *pressão arterial*

```
{
  "patient_id": "AX-TEST-0001",
  "encounter_id": "enc_d0_0001",
  "type": "blood-pressure",
  "status": "final",
  "effective_at": "2026-08-21T09:10:00-03:00",
  "components": [
    {"code": "8480-6", "value": 145, "unit": "mm[Hg]"},
    {"code": "8462-4", "value":  92, "unit": "mm[Hg]"}
  ],
  "context": {"position": "sitting", "rested_5min": true},
  "author": {"user_id": "usr_nurse_01", "role": "nurse"}
}
```

NA PRÁTICA Dado sintético sempre. Nunca usar dado identificável de paciente em staging, tickets, prompts de IA ou capturas de tela.

SEÇÃO 9.4

Retificação, passo a passo

PASSO	COMPORTAMENTO ESPERADO
1. Identificar erro	usuário autorizado abre “retificar”; o sistema não habilita edit in place
2. Justificar	motivo obrigatório; dado sensível não deve aparecer em log técnico
3. Criar versão	novo registro com supersedes_id, novo timestamp e novo autor
4. Exibir	a UI mostra a versão atual e sinaliza histórico; o auditor encontra ambas
5. Exportar	o documento indica a retificação sem apagar o original

NA PRÁTICA Este é o fluxo que separa um prontuário de uma planilha. Implemente-o antes de qualquer tela bonita.

SEÇÃO 10.1

Princípios de *UX clínica*

- Patient banner persistente: identidade, alergia crítica, alertas relevantes, contexto do encounter e ambiente.
- Disclosure progressivo: mostrar primeiro o necessário para decidir; detalhe sob demanda, sem esconder risco.
- Workspace de entrada separado da timeline. Salvar draft não é finalizar.
- Unidades e método junto ao valor: “145/92” sem posição, data e autoria é informação incompleta.
- Alertas informam risco e ação; excesso de vermelho cria fadiga e deixa de proteger.
- Acessibilidade: teclado, contraste, foco, rótulos, leitura de erro — nunca depender só de cor.
- Erro de rede: manter draft seguro, evitar duplicação e nunca exibir sucesso falso.

NA PRÁTICA Referências públicas (OpenEMR, LifeOmic) servem para discutir hierarquia de informação — não para copiar aparência.

SEÇÃO 11.1

Fatia vertical mínima *para a primeira demo*

- 1. Autenticar como enfermagem em staging e localizar paciente sintético por nome ou ID.
- 2. Abrir D0, confirmar identidade e registrar PA, FC, peso, altura e ECG/anexo.
- 3. Acionar soft alert por PA elevada sem bloquear o draft; exigir ação para finalizar.
- 4. Finalizar encounter com autor, papel, data/hora, versão do checklist e status do marco.
- 5. Abrir a timeline como médico e ver o evento sem poder alterar a nota da enfermagem.
- 6. Retificar um valor e comprovar a preservação das duas versões e do AuditEvent.
- 7. Exportar PDF legível do episódio e JSON/FHIR dos sinais vitais essenciais.

NA PRÁTICA Esta é a demo que prova o produto inteiro. Se ela funciona ponta a ponta, o resto é volume.

SEÇÃO 11.2

Testes que *bloqueiam o go-live*

ID	CENÁRIO	RESULTADO ESPERADO
T-01	Enfermagem tenta editar nota médica final	negado no servidor; evento auditado
T-02	Clínica A usa ID de paciente da clínica B	404/403 sem vazamento; teste automatizado
T-03	D14 sem classificação	salva draft; não fecha como completed
T-04	PAD ≥ PAS	erro explícito; valor inválido não finaliza
T-05	Anexo executável renomeado como PDF	bloqueado ou colocado em quarentena
T-06	Falha após clique em salvar	sem sucesso falso; idempotência evita duplicata
T-07	Alterar o relógio do cliente	servidor mantém recorded_at confiável
T-08	Retificar PA final	original preservado; nova versão ligada
T-09	Restaurar backup	dados e anexos recuperados; integridade verificada
T-10	Exportar prontuário	legível, com autoria, datas e retificações
T-11	Log de erro em endpoint clínico	sem conteúdo clínico, token ou CPF completo
T-12	Revogar usuário	sessões invalidadas e novo acesso bloqueado

SEÇÃO 11.3

Definition of Done

- Critério de aceite demonstrado com paciente sintético em staging.
- Teste automatizado para regra determinística e teste manual para fluxo clínico.
- Autorização e isolamento revisados.
- Migração e rollback considerados.
- Observabilidade sem PHI desnecessária.
- Documentação de API e de modelo atualizada.
- Aceite clínico pela responsável designada.
- Nenhum blocker de segurança ou compliance aberto.

NA PRÁTICA Requisito sem teste e sem evidência não está concluído. Sem exceção, sem “depois”.

SEÇÃO 12

Backlog por *gates G0–G6*

GATE	ENTREGAS	SAÍDA OBJETIVA
G0 · decisões	fonte oficial, custódia, papéis, assinatura, retenção, cloud e regiões, intended use	ADR + matriz jurídica aprovadas
G1 · fundação	auth, tenant, RBAC, paciente, encounter, audit, anexos, observabilidade	testes SEC-01/02/06/09 passam
G2 · Core clínico	segurança, notas, vitais, timeline, agenda, exportação, backup e restore	fluxo avulso completo sem legado
G3 · Pathway	pacote, marcos, D0/D30, D14/D21, multi, metas, dossiê, KPI	paciente sintético D0–D30 completo
G4 · piloto	migração mínima, treinamento, suporte, contingência, piloto controlado	casos reais autorizados com monitoramento
G5 · cutover	legado read-only ou desligado conforme plano; operação só no AXIS	go/no-go assinado e rollback pronto
G6 · escala	portal do paciente, interoperabilidade, certificação/pentest e expansão	métricas e riscos sustentam a expansão

SEÇÃO 12.1

O que fica *fora do MVP*

- Pathway de outra especialidade.
- IA que diagnostica ou prescreve.
- Integrações oportunistas sem caso de uso e sem contrato.
- Dashboard executivo antes da confiabilidade do dado.
- Customização por cliente que quebra o Core.
- Automação de marketing com dados de saúde sem governança.

POR QUE ISSO IMPORTA

Escopo negado por escrito é escopo que não volta pela porta dos fundos no meio da sprint. Esta lista protege a data de entrega tanto quanto protege o paciente.

SEÇÃO 13.1

Go-live: *evidências obrigatórias*

PACOTE DE EVIDÊNCIA	CONTEÚDO
Produto	escopo do MVP, fluxos, critérios de aceite e exclusões
Clínico	protocolos versionados, responsáveis e fluxo de escalonamento
Jurídico / privacidade	bases e finalidades, contratos, avisos, direitos, retenção, incidentes e transferência
Segurança	threat model, testes, scans, pentest conforme gate, matriz de acesso e logs
Operação	treinamento, suporte, backup/restore, downtime, migração, rollback e responsáveis
Tecnologia	ADR, modelo de dados, API, versionamento, monitoramento e runbooks

SEÇÃO 13.2

Três decisões sem as quais *a reunião não termina*

1 · Fonte oficial e cutover

Qual fluxo e conjunto de dados tornam o AXIS o prontuário oficial do MVP, o que acontece com o legado e como o aceite será comprovado.

2 · Barra de segurança e dono

Quais controles bloqueiam produção, quem responde por cada evidência e qual instância decide go/no-go.

3 · Primeira fatia vertical e data

Um fluxo ponta a ponta — recomendação: D0 de enfermagem até timeline médica e retificação — com data de demo, stories e critérios de aceite.

NA PRÁTICA Registrar decisão, owner, prazo e evidência. Decisão sem dono é pendência disfarçada.

APÊNDICE A

Checklist técnico *por domínio*

ID	NÍVEL	REQUISITO
DATA-01	MUST	Cada Observation tem patient_id, effective_at, unit, author e encounter quando aplicável.
DATA-02	MUST	Dados de D30 criam novo evento; não sobrescrevem D0.
DATA-03	MUST	ChecklistResponse preserva a versão do questionário.
DATA-04	MUST	Fusão de paciente duplicado preserva identificadores e trilha.
DATA-05	MUST	Enums clínicos têm catálogo e versionamento; “outro” exige texto.
APP-01	MUST	Todo comando de escrita é idempotente ou protegido contra duplo envio.
APP-02	MUST	Mudança de esquema é backward-compatible durante deploy e rollback.
APP-03	MUST	Feature flag não pode contornar autorização ou consistência.
UX-01	MUST	Alergia crítica e identidade permanecem visíveis no contexto clínico.
UX-02	MUST	Draft, final e amended têm aparência inequívoca.
UX-03	MUST NOT	Usar cor como único indicador de status ou risco.
UX-04	MUST	A finalização exibe resumo e confirma a consequência.

APÊNDICE B

Fontes oficiais *e técnicas*

R1 CFM — Resolução 1.638/2002

R2 CFM — Resolução 1.821/2007

R3 Lei 13.787/2018

R4 LGPD — Lei 13.709/2018

R5 CFM 2.314/2022 — Telemedicina

R6 Cofen 696/2022 — Telenfermagem

R7 Cofen 754/2024 — Prontuário eletrônico

R9 ANPD — Comunicação de incidentes (Res. 15/2024)

R10 ANPD — Transferência internacional (Res. 19/2024)

R11 SBIS — Requisitos PEP v5.2

R12 Anvisa — SaMD / RDC 657/2022

R13 HL7 FHIR R4 — Vital Signs

R15 OWASP ASVS

R16 Ministério da Saúde — RNDS

• ENCERRAMENTO

No fim, tudo isto existe *por uma pessoa só*

Cada regra deste manual nasceu de uma cena de consultório: um exame que sumiu, uma nota sem autor, um retorno que não aconteceu, uma pessoa que saiu da sala sem entender o próprio coração. Escrever software de saúde é transformar cuidado em estrutura — e estrutura em confiança.

O COMPROMISSO

Construir devagar onde é preciso ser seguro, e rápido onde é preciso ser útil. Nenhum evento se perde. Nenhum autor desaparece. Nenhum paciente fica sem entender o que foi combinado.