

Checklist de implantação do prontuário eletrônico AXIS

Passo a passo para clínicas médicas — anexo operacional do manual técnico-jurídico

Anexo v1.0 · derivado do manual v1.1 (26 de agosto de 2026)

Este anexo é material de trabalho. Não substitui parecer jurídico, certificação SBIS, avaliação independente de segurança nem as regras internas da clínica. Cada item só é considerado concluído quando existe evidência escrita, com responsável e data.

G0 Decisões que abrem o projeto

Saída objetiva: ADR e matriz jurídica aprovadas. Sem isto, não se escreve código de produção.

- | | |
|--|--------------|
| ☐ G0-01 Definir qual fluxo e qual conjunto de dados tornam o AXIS o prontuário oficial da clínica. | Resp. / data |
| Evidência: ADR de fonte oficial assinada pela direção clínica | |
| ☐ G0-02 Definir o destino do prontuário legado: leitura, migração parcial ou desligamento, e em que data. | Resp. / data |
| Evidência: Plano de cutover com datas | |
| ☐ G0-03 Nomear responsáveis: custódia do prontuário, encarregado de dados, dono da segurança e aprovador clínico. | Resp. / data |
| Evidência: Matriz de responsabilidades nominal | |
| ☐ G0-04 Definir política de retenção e descarte, tomando como piso de referência 20 anos após o último registro. | Resp. / data |
| Evidência: Política de retenção aprovada | |
| ☐ G0-05 Decidir a estratégia de assinatura e a viabilidade de operação sem papel antes de construir o fechamento de documentos. | Resp. / data |
| Evidência: Decisão formal sobre assinatura e paperless | |
| ☐ G0-06 Declarar o intended use do sistema e verificar se alguma funcionalidade o aproxima de software como dispositivo médico. | Resp. / data |
| Evidência: Declaração de intended use e análise de enquadramento | |
| ☐ G0-07 Definir nuvem, regiões e eventuais transferências internacionais de dados. | Resp. / data |
| Evidência: ADR de infraestrutura e regiões | |

G1 Fundação técnica

Saída objetiva: os testes de segurança da fundação passam em ambiente controlado.

- | | |
|--|--------------|
| ☐ G1-01 Autenticação com sessão controlada, revogação imediata e segundo fator para perfis privilegiados. | Resp. / data |
| Evidência: Teste de revogação de usuário aprovado | |

☐	G1-02 Isolamento multi-tenant garantido no servidor: nenhuma clínica alcança dados de outra por manipulação de ID. Evidência: Teste automatizado de isolamento	Resp. / data
☐	G1-03 Autorização por papel profissional decidida no servidor. Esconder botão na interface não é controle de acesso. Evidência: Matriz de acesso e testes por papel	Resp. / data
☐	G1-04 Cadastro de paciente e de encounter com autoria, papel, data do fato e data do registro. Evidência: Modelo de dados revisado	Resp. / data
☐	G1-05 Trilha de auditoria imutável para leitura, criação, retificação, exportação e ações privilegiadas. Evidência: Amostra de log auditado	Resp. / data
☐	G1-06 Anexos com verificação de tipo, limite de tamanho, varredura e armazenamento privado. Evidência: Teste de anexo executável renomeado	Resp. / data
☐	G1-07 Observabilidade sem conteúdo clínico, token ou documento completo nos logs de erro. Evidência: Revisão de logs de erro	Resp. / data

G 2 Core clínico

Saída objetiva: um atendimento avulso completo dentro do AXIS, sem depender do legado.

☐	G2-01 Registro de sinais vitais com unidade, contexto e validação explícita de valores impossíveis. Evidência: Testes de validação de PA	Resp. / data
☐	G2-02 Notas clínicas com rascunho e versão final; nota final de um profissional não é editável por outro. Evidência: Teste de edição negada no servidor	Resp. / data
☐	G2-03 Retificação não destrutiva: a versão original é preservada e vinculada à nova. Evidência: Teste de retificação com histórico	Resp. / data
☐	G2-04 Linha do tempo do paciente legível, com autoria, papel e data de cada evento. Evidência: Aceite clínico da timeline	Resp. / data
☐	G2-05 Exportação do prontuário legível, com autoria, datas e retificações visíveis. Evidência: Exportação de paciente sintético	Resp. / data
☐	G2-06 Backup automatizado, separado e criptografado, com restauração testada de ponta a ponta. Evidência: Relatório de restore drill	Resp. / data

G 3 Jornada cardiovascular

Saída objetiva: um paciente sintético percorre D0 a D30 completo.

☐	G3-01 Pacote de cuidado com marcos D0, D14, D21, D30 e D90 e responsáveis por marco. Evidência: Protocolo versionado	Resp. / data
☐	G3-02 Registro multiprofissional no mesmo paciente sem sobreposição de autoria. Evidência: Simulação com enfermagem, medicina e nutrição	Resp. / data

☐	G3-03 Portão clínico: o marco não fecha sem os dados obrigatórios definidos pelo protocolo. Evidência: Teste de fechamento bloqueado	Resp. / data
☐	G3-04 Metas e indicadores do pacote calculados a partir do dado registrado, não digitados à parte. Evidência: Conferência de indicadores	Resp. / data
☐	G3-05 Dossiê do paciente pronto para entrega ao titular, sem dados de terceiros. Evidência: Amostra de dossiê revisada	Resp. / data

G 4 Piloto controlado na clínica

Saída objetiva: casos reais autorizados, com monitoramento e plano de contingência ativo.

☐	G4-01 Treinamento da equipe por papel, com material escrito e registro de participação. Evidência: Lista de presença e material	Resp. / data
☐	G4-02 Migração mínima definida: o que entra, o que fica no legado e como o profissional consulta o histórico. Evidência: Plano de migração aprovado	Resp. / data
☐	G4-03 Plano de contingência para indisponibilidade: como registrar e como reconciliar sem duplicar. Evidência: Procedimento de contingência afixado	Resp. / data
☐	G4-04 Canal de suporte com tempo de resposta acordado durante o piloto. Evidência: Acordo de suporte	Resp. / data
☐	G4-05 Ambiente de homologação separado, sem cópia bruta de dados de pacientes reais. Evidência: Evidência de dados sintéticos	Resp. / data

G 5 Cutover e operação oficial

Saída objetiva: go/no-go assinado e plano de rollback pronto.

☐	G5-01 Legado em somente leitura ou desligado conforme o plano, com data e responsável. Evidência: Registro de cutover	Resp. / data
☐	G5-02 Operação assistencial acontecendo exclusivamente no AXIS para o escopo definido. Evidência: Auditoria de uso na primeira semana	Resp. / data
☐	G5-03 Nenhum bloqueador de segurança ou privacidade em aberto na data do go-live. Evidência: Ata de go/no-go	Resp. / data
☐	G5-04 Rollback documentado: o que acontece se for necessário voltar atrás e quem decide. Evidência: Plano de rollback	Resp. / data

G 6 Escala e amadurecimento

Saída objetiva: métricas e riscos sustentam a expansão para novas unidades.

☐	G6-01 Portal do paciente liberado com controle de acesso e conteúdo revisado. Evidência: Aceite clínico do portal	Resp. / data
--------------------------	---	--------------

☐	G6-02 Interoperabilidade avaliada caso a caso, com contrato e caso de uso definidos. Evidência: Contrato de integração	Resp. / data
☐	G6-03 Teste de intrusão realizado e correções priorizadas por severidade. Evidência: Relatório de pentest e plano de correção	Resp. / data
☐	G6-04 Decisão formal sobre buscar certificação, com responsável e prazo. Evidência: Ata de decisão	Resp. / data

L G P D

Privacidade e governança — verificação contínua

Deve ser revisto a cada trimestre e sempre que um novo tratamento de dados for criado.

☐	PRIV-01 Mapa de tratamentos atualizado: finalidade, base legal, dados, retenção e compartilhamento. Evidência: Registro de operações de tratamento	Resp. / data
☐	PRIV-02 Contratos com fornecedores que tratam dados de saúde, com cláusulas de proteção e subcontratação. Evidência: Contratos assinados	Resp. / data
☐	PRIV-03 Canal e prazo para atendimento aos direitos do titular, sem expor dados de terceiros. Evidência: Procedimento publicado	Resp. / data
☐	PRIV-04 Procedimento de resposta a incidente com prazos, responsáveis e critério de comunicação. Evidência: Plano de resposta a incidentes	Resp. / data
☐	PRIV-05 Proibição operacional confirmada: nenhum dado identificável em homologação, chamados, capturas de tela ou ferramentas de IA. Evidência: Norma interna comunicada à equipe	Resp. / data

Encerramento do checklist

O checklist só é considerado concluído quando as quatro assinaturas abaixo existem para o escopo declarado no gate G0.

Responsável clínico — nome, assinatura e data

Responsável técnico — nome, assinatura e data

Encarregado de dados — nome, assinatura e data

Direção da clínica — nome, assinatura e data