



KLINIKSYS / GOVERNANÇA E PRIVACIDADE

Política de Privacidade e Termos de Uso, KlinikSys

Política de Privacidade

CÓDIGO	KS-LGP-005	VERSÃO	1.1
VIGÊNCIA	16/09/2026	PRÓXIMA REVISÃO	Anual
CLASSIFICAÇÃO	Público	PROPRIETÁRIO	Segurança e Privacidade

USO E CONFIDENCIALIDADE

Público. Pode ser compartilhado livremente.

Sumário

1 Quem somos	3
2 Quais dados tratamos	3
2.1 Do paciente (dato sensível, Art. 5º, II LGPD)	3
2.2 Do profissional de saúde (dato pessoal, Art. 5º, I LGPD)	3
2.3 Operacionais	3
3 Base legal e finalidade	4
3.1 Paciente	4
3.2 Profissional	4
4 Compartilhamento	4
5 Direitos do titular (Art. 18 LGPD)	5
6 Retenção de dados	5
7 Segurança	6
8 Cookies e armazenamento local	6
9 Crianças	7
10 Transferência internacional	7
11 Alterações	7
12 Contato	7

Última atualização: 2026-09-16 (v1.2)

NOTA

Análise jurídica fundamentada por artigo em LGPD_COMPLIANCE.md. Este documento é a versão pública para o titular. Para encarregado, auditor ou jurídico, ler também DPIA.md, ROPA.md e SECURITY_LGPD_AUDIT.md.

NOTA

Este documento é um **modelo**. Antes de produção com dados reais, revisar com assessoria jurídica especializada em LGPD e saúde e preencher nome do controlador, contato do encarregado, endereço e CNPJ.

NOTA

Revisão de 16/09/2026. A versão anterior afirmava contrato de tratamento firmado com o Supabase, fluxo de consentimento implementado para profissionais e expiração de sessão por inatividade, nenhum dos três verdadeiro, e marcava como planejadas medidas que já estavam em uso. Também omitia operadores. Tudo foi conferido contra o código e a configuração publicada nesta data.

1 Quem somos

O **KlinikSys** é um sistema de prontuário eletrônico operado por **[NOME DA ORGANIZAÇÃO]** (controladora), responsável pelo tratamento de dados pessoais e sensíveis na forma desta política.

- **Encarregado de Dados (DPO):** [nome], [email]
- **Endereço:** [endereço completo da organização]
- **CNPJ:** [CNPJ]

2 Quais dados tratamos

2.1 Do paciente (dado sensível, Art. 5º, II LGPD)

Nome, apelido, data de nascimento, sexo, nome da mãe, CPF, RG, contato (telefone ou WhatsApp), endereço, comunidade, referência familiar, foto, histórico médico (alergias, doenças crônicas, medicação contínua), consultas, diagnósticos, prescrições, exames solicitados e sinais vitais.

Não coletamos e-mail do paciente.

2.2 Do profissional de saúde (dado pessoal, Art. 5º, I LGPD)

Nome, e-mail, número de registro no conselho (CRM, COREN, CRO), especialidade, foto (opcional), imagem da assinatura, papel no sistema, organização, vínculo de voluntário e sua validade, e registros de acesso.

2.3 Operacionais

Trilha de auditoria (quem acessou o quê, quando), registros técnicos de erro sem dados de paciente, backups locais cifrados e fila de sincronização offline.

3 Base legal e finalidade

3.1 Paciente

- **Base legal:** Art. 11, II, alínea "f" da LGPD, *"tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária"*
- **Por que essa hipótese e não consentimento?** O atendimento em comunidade ribeirinha frequentemente envolve titulares vulneráveis (analfabetismo, hipossuficiência). Nesse contexto, a tutela da saúde por profissional é base mais protetiva que o consentimento. O profissional orienta verbalmente sobre o tratamento.
- **Salvaguardas:**
 - Não usamos dado de saúde para vantagem econômica: sem anúncios, sem venda, sem compartilhamento comercial.
 - Medidas técnicas: isolamento por organização (RLS), cache e backup locais cifrados (AES-GCM 256), MFA obrigatório para administradores, trilha de auditoria, arquivos privados com link temporário e bloqueio de tela por inatividade.
 - **Finalidade:** atendimento médico, odontológico, de enfermagem, vacinação e triagem; rastreo epidemiológico da comunidade; gestão de prontuário; prescrição; acompanhamento longitudinal.
 - **Crianças e adolescentes:** tratados com a mesma base (Art. 11, II, "f"), observado e prevalecente o seu melhor interesse (Art. 14 e Enunciado CD/ANPD nº 1/2023). O atendimento é sempre feito por profissional de saúde habilitado.

3.2 Profissional

- **Base legal dos campos necessários à operação clínica:**
 - Nome e número de registro no conselho -> **Art. 7º, II** (obrigação legal de identificar o profissional responsável pelo atendimento)
 - E-mail (autenticação), papel (controle de acesso) e organização -> **Art. 7º, IX** (legítimo interesse na operação do sistema)
- **Base legal dos campos opcionais:**
 - Foto -> **Art. 7º, I** (consentimento). O registro desse consentimento **ainda não está implementado** no sistema.
 - **Imagem da assinatura:** desde 25/08/2026 os documentos impressos saem sem assinatura estampada, e o profissional assina à mão no papel. A necessidade de manter a imagem armazenada está em reavaliação.
 - **Finalidade:** controle de acesso, identificação do profissional responsável e auditoria.
 - **Revogação:** o profissional pode pedir a retirada da foto a qualquer momento, pelo e-mail do encarregado. Nome e registro permanecem enquanto houver prontuário associado dentro do prazo de guarda (20 anos).

4 Compartilhamento

Não vendemos dados. Compartilhamos com os operadores abaixo. Os contratos de tratamento com eles **ainda não foram formalizados**; enquanto isso, valem os termos padrão de cada fornecedor.

Sempre em uso:

- **Supabase Inc.**, banco de dados, autenticação e arquivos. Servidores em São Paulo (sa-east-1).
- **Vercel Inc.**, hospedagem dos arquivos do aplicativo. Não recebe dados de paciente.
- **Resend Inc.**, envio dos e-mails de acesso dos profissionais (confirmação, convite, redefinição de senha). Recebe apenas o e-mail do profissional; guarda o conteúdo por 3 dias.
- **Sentry (Functional Software, Inc.)**, monitoramento de erros do sistema, quando habilitado na publicação do aplicativo. Os dados de paciente são removidos antes do envio; recebe o identificador do profissional logado.

Somente se a organização ativar o recurso (desligados por padrão):

- **Google LLC**, IA de apoio à decisão clínica e transcrição de consulta. A análise envia data de nascimento, sexo, histórico médico, sinais vitais e o relato da queixa, sem nome, CPF ou foto; a transcrição envia o áudio da consulta.

Autoridades públicas, quando exigido por ordem judicial ou obrigação legal.

5 Direitos do titular (Art. 18 LGPD)

Qualquer paciente pode solicitar gratuitamente:

Direito	Como pedir
Confirmação e acesso aos dados	E-mail ao encarregado
Correção de dados incorretos	Solicitar à equipe clínica
Anonimização ou bloqueio de dados desnecessários	E-mail ao encarregado
Portabilidade	E-mail ao encarregado, entregue em JSON em até 15 dias
Eliminação dos dados tratados com consentimento	E-mail ao encarregado
Informação sobre compartilhamento	Esta política
Revogação do consentimento	E-mail ao encarregado
Oposição ao tratamento	E-mail ao encarregado

Prazo de resposta: 15 dias corridos.

Limitação importante: dados clínicos de prontuário seguem a guarda mínima de 20 anos (Resolução CFM 1.821/2007 e Lei 13.787/2018) e podem ser mantidos mesmo após pedido de eliminação. Nesses casos, oferecemos **anonimização** em vez de exclusão completa.

6 Retenção de dados

Prazos da Política de Retenção e Descarte:

Categoria	Prazo
Prontuário (paciente e atendimentos)	No mínimo 20 anos do último registro (Res. CFM 1.821/2007; Lei 13.787/2018)
Trilha de auditoria	No mínimo 5 anos
Logs técnicos de aplicação	90 dias
Registros de tentativa de login	6 meses
Conta de profissional desligado	Bloqueio imediato; o registro de acesso é preservado pela trilha de auditoria
E-mails de acesso na Resend	3 dias
Backup exportado pela organização	Definido pela organização
Dispensação de medicamentos	A definir com o encarregado

Após o prazo do prontuário, a organização identifica por relatório os registros vencidos e executa a anonimização. Não há expurgo automático no banco.

7 Segurança

Medidas adotadas:

- **HTTPS sempre**, com HSTS
- **MFA** obrigatório para administradores
- **Senha forte**: mínimo de 8 caracteres, 12 para administradores e gestores, com checagem contra senhas vazadas
- **Limite de tentativas de login** por endereço de rede
- **Cache local cifrado** com chave derivada da senha do profissional (AES-GCM 256)
- **Arquivos de fotos e assinaturas privados**, acessados por link temporário de 1 hora
- **Isolamento entre organizações** no banco (RLS)
- **Trilha de auditoria** das ações relevantes (visualização, criação, edição, exclusão, exportação)
- **Bloqueio de tela** após 15 minutos de inatividade, que descarta a chave de cifra do cache até a senha ser digitada novamente
- **Voluntário** com data de validade pode ter o acesso encerrado ao fim do prazo
- **Backup local cifrado**
- **Comunicação à ANPD** em até 3 dias úteis em caso de incidente com risco relevante (Art. 48; Res. CD/ANPD 15/2024)

8 Cookies e armazenamento local

- **IndexedDB**: cache cifrado de pacientes e fila de sincronização (essencial ao funcionamento sem internet). Não usamos ferramentas de análise de comportamento de terceiros.

- **localStorage:** idioma, tema (claro ou escuro), última sincronização.
- **Service Worker:** cache de fotos de pacientes e de mapas para funcionamento sem internet.

9 Crianças

O sistema atende crianças (pediatria). Os dados de menores são tratados com a mesma base legal de tutela da saúde (Art. 11, II, "f"), observado e prevalecente o seu melhor interesse (Art. 14 e Enunciado CD/ANPD nº 1/2023). Não há oferta direta a crianças nem coleta sem profissional de saúde envolvido.

10 Transferência internacional

Os dados em repouso ficam em **São Paulo (sa-east-1)**. A hospedagem do aplicativo pode rotear requisições por outros países, mas não recebe dados de paciente.

Há envio para fora do Brasil nestes casos:

- **Monitoramento de erros (Sentry),** quando habilitado, sem dados de paciente.
- **E-mails de acesso (Resend):** o envio é feito em São Paulo; a localização dos registros de 3 dias ainda não foi confirmada com o fornecedor.
- **Recursos opcionais, desligados por padrão:** IA e transcrição (Google, EUA).

A organização que não quiser transferência internacional de dado de paciente simplesmente não ativa os recursos opcionais. O atendimento funciona sem eles.

11 Alterações

Esta política pode ser atualizada. Mudanças relevantes serão comunicadas no próximo login do profissional e ao paciente pela equipe clínica, quando aplicável.

12 Contato

Encarregado de Dados: **[email]**

Reclamações também podem ser feitas diretamente à ANPD em www.gov.br/anpd.

CONTROLE DE DISTRIBUIÇÃO

A versão vigente deve permanecer no repositório oficial da KlinikSys. Impressões e arquivos exportados não são controlados; valide sempre o código e a versão antes do uso.

CÓDIGO	KS-LGP-005	VERSÃO	1.1
CLASSIFICAÇÃO	Público	PROPRIETÁRIO	Segurança e Privacidade
APROVADOR	Proprietário do produto	PRÓXIMA REVISÃO	Anual

FIM DO DOCUMENTO