Aura Onco
Plataforma de organização e acompanhamento do cuidado oncológico

DOCUMENTO LEGAL · LGPD

Política de Privacidade

Quais dados pessoais tratamos, para quê, com quem compartilhamos, onde ficam, por quanto tempo e como você exerce os seus direitos.

Versão 1.9 · vigente desde 18 de outubro de 2026
auraonco.com/privacidade

Aura Health Ltda.
CNPJ 67.652.854/0001-23

Nesta política

Cada item leva direto à seção.

01 Introdução

02 Quem somos (Controlador dos dados)

03 Definições

04 Princípios que seguimos

05 Quais dados coletamos e com quais finalidades

06 Uso de inteligência artificial na leitura de documentos

07 Bases legais

08 Dados sensíveis de saúde

09 Dados de menores e adolescentes

10 Compartilhamento e operadores (subprocessadores)

11 Pesquisa clínica e científica

12 Comunicações de marketing

13 Transferência internacional

14 Segurança da informação

15 Prazo de retenção

16 Cookies e tecnologias semelhantes

17 Links de terceiros

18 Seus direitos como titular

19 Farmacovigilância e eventos adversos

20 Encarregado (DPO) e contato

21 Alterações nesta Política

22 Legislação aplicável

SEÇÃO 01

Introdução

A jornada de quem enfrenta o câncer exige confiança. Por isso, na Aura Health Ltda. (“Aura”, “nós”), proteger seus dados pessoais — em especial seus dados de saúde — é uma prioridade e uma condição para a existência da nossa plataforma.

Esta Política de Privacidade (“Política”) explica, de forma transparente, quais dados pessoais tratamos por meio das Plataformas Aura, com quais finalidades, com base em quais fundamentos legais, com quem eventualmente os compartilhamos, por quanto tempo os mantemos e como você pode exercer seus direitos, tudo em conformidade com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais — “LGPD”) e demais normas aplicáveis.

Ao criar uma conta e utilizar o aplicativo do paciente ou o painel clínico, você declara ter lido e compreendido esta Política. Recomendamos que você a consulte periodicamente; alterações relevantes serão comunicadas conforme a seção “Alterações nesta Política”.

SEÇÃO 02

Quem somos (Controlador dos dados)

O responsável pelas decisões de tratamento dos seus dados pessoais no âmbito das Plataformas Aura é:

Campo	Valor
RAZÃO SOCIAL	AURA HEALTH LTDA
CNPJ	67.652.854/0001-23
NOME FANTASIA	Aura Health / Aura Saúde
ENDEREÇO	Rua Paraná, nº 2781, Sala 2, Centro, Cascavel/PR, CEP 85.812-011
ENCARREGADO (DPO)	Matheus Celso Fachim dos Santos
CONTATO DO ENCARREGADO	privacidade@auraonco.com

As Plataformas Aura compreendem: (i) o aplicativo móvel do paciente (Android e iOS); (ii) o painel clínico web destinado a profissionais de saúde, clínicas e hospitais; e (iii) os sites institucionais do Grupo Aura (auraonco.com e groupaura.com.br).

SEÇÃO 03

Definições

Para facilitar a leitura, adotamos as definições da LGPD, entre elas:

- **Dados Pessoais:** qualquer informação relacionada a pessoa natural identificada ou identificável (ex.: nome, CPF, e-mail, telefone).
- **Dados Pessoais Sensíveis:** dados sobre saúde, origem racial ou étnica, dado genético ou biométrico, vida sexual, entre outros. Os dados clínicos tratados na Aura são, em regra, dados sensíveis de saúde.
- **Titular:** a pessoa natural a quem os dados se referem (paciente, cuidador ou profissional de saúde).
- **Tratamento:** qualquer operação com dados pessoais (coleta, armazenamento, uso, compartilhamento, eliminação etc.).
- **Controlador:** a Aura, quando decide sobre as finalidades e os meios do tratamento.
- **Operador:** terceiro que trata dados em nome da Aura (ex.: provedores de infraestrutura).
- **Cuidador:** pessoa autorizada pelo paciente a acompanhar seu cuidado no aplicativo.
- **Equipe de Saúde / Equipe Médica:** profissionais de saúde vinculados à clínica ou hospital que atende o paciente e que utilizam o painel clínico.
- **ANPD:** Autoridade Nacional de Proteção de Dados.

SEÇÃO 04

Princípios que seguimos

Tratamos seus dados de acordo com os princípios da LGPD: finalidade, adequação, necessidade (coletamos o mínimo necessário), livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização. Adotamos o princípio da minimização como padrão de projeto (privacy by design): funcionalidades são construídas para usar a menor quantidade de dados possível.

SEÇÃO 05

Quais dados coletamos e com quais finalidades

Coletamos dados que você nos fornece diretamente, dados gerados pelo seu uso da plataforma e dados extraídos de documentos que você opta por enviar. A tabela a seguir resume os principais tratamentos:

A quem se aplica	Atividade	Dados tratados	Finalidade
Paciente / Responsável legal	Criação de conta e cadastro	Nome, data de nascimento, CPF, telefone, e-mail, cidade, sexo	Identificar o usuário, verificar idade, autenticar acesso e prestar o serviço
Paciente	Registro clínico (sensível)	Sintomas e intensidade, medicamentos em uso, reações adversas a medicamentos, exames, peso, sono, humor, diagnóstico e tipo de tumor	Organizar e acompanhar o cuidado do paciente e permitir que a equipe de saúde vinculada o acompanhe
Paciente	Envio de documentos e OCR	Imagens e PDFs de laudos, receitas e exames; texto extraído por OCR	Estruturar e centralizar o histórico do paciente a partir dos documentos enviados

A quem se aplica	Atividade	Dados tratados	Finalidade
Paciente	Agenda e lembretes	Consultas, datas de medicação e exames incluídos na agenda do app	Enviar lembretes ao dispositivo do paciente
Paciente	Login social	Nome, e-mail e identificador de conta fornecidos pelo provedor de login (Google), quando você opta por entrar por esse meio	Autenticar o acesso de forma simplificada
Cuidador	Cadastro e vinculação	Nome, e-mail/telefone e vínculo autorizado com o paciente	Permitir acompanhamento autorizado pelo paciente
Profissional de saúde	Acesso ao painel clínico	Nome, e-mail corporativo, registro profissional, instituição, papel/permissões	Autenticar o profissional e controlar o acesso aos dados dos pacientes vinculados
Todos	Uso técnico e segurança	Endereço IP, identificadores de dispositivo, logs de acesso e eventos, dados de desempenho	Garantir segurança, prevenir fraudes, corrigir falhas e melhorar a plataforma

Observação: o painel clínico aplica controle de acesso por papel e mascaramento de dados sensíveis (ex.: CPF/PII) conforme o perfil do profissional.

SEÇÃO 06

Uso de inteligência artificial na leitura de documentos

Você decide se uma ferramenta de inteligência artificial pode ler o documento que você envia, a foto ou o PDF de um exame. Quando você autoriza, ela adianta o preenchimento dos valores, para que ninguém precise digitar um hemograma linha a linha. Sem a sua autorização, o documento é só guardado.

- **O que ela faz:** transcreve o que está escrito no documento — nome do exame, data, valores e unidades. É leitura, não interpretação.
- **O que ela não faz:** não emite laudo, não dá diagnóstico e não decide nada sobre o seu tratamento. Enquanto um profissional não conferir, o valor aparece marcado no sistema como não conferido.
- **Quem processa:** Anthropic, como operadora, nos Estados Unidos. O documento é enviado íntegro — ele precisa ser lido inteiro para ser transcrito — e os valores lidos passam por uma segunda leitura, feita por outro modelo da mesma empresa, que só aponta o que conferir. A Anthropic não usa o conteúdo para treinar modelos e o apaga em até 30 dias, salvo quando precisa guardá-lo por mais tempo para apurar abuso ou por obrigação legal. A OpenAI, também nos Estados Unidos, fica como reserva desligada, para o caso de a Anthropic ficar indisponível.
- **O que fica registrado:** cada leitura guarda quando aconteceu, qual modelo leu, o que ele leu, quem conferiu depois e o que foi alterado na conferência. Esse registro pode ser emitido em PDF e anexado ao prontuário da instituição.
- **Como autorizar e como mudar de ideia:** a leitura vem desligada e só acontece depois que você autoriza. O aplicativo pergunta na tela “Sua privacidade” do cadastro e, a quem ainda não respondeu, antes de adicionar o primeiro documento; a pergunta avisa que o documento, que é dado de saúde, será enviado a

provedores de inteligência artificial fora do Brasil (como os Estados Unidos). Se você não autoriza, o documento é guardado sem leitura, com o nome e a data que você informar, e os valores são preenchidos à mão. Você muda de ideia quando quiser em Ajustes › Privacidade, na chave "Leitura automática dos exames por IA": ligada, vale para os envios seguintes; desligada, os próximos documentos não são enviados para leitura. Guardamos a data em que você autorizou ou recusou, e o servidor confere a sua escolha antes de cada envio ao provedor: se não conseguir confirmá-la, o documento não é enviado.

SEÇÃO 07

Bases legais

Cada tratamento tem uma base legal específica da LGPD. As principais são:

- **Consentimento (art. 7º, I, e art. 11, I):** para o tratamento de dados sensíveis de saúde registrados por você e para a vinculação do seu registro à sua equipe de saúde. O consentimento é coletado de forma destacada e pode ser revogado a qualquer momento.
- **Execução de contrato (art. 7º, V):** para prestar as funcionalidades que você contratou ao criar a conta.
- **Tutela da saúde (art. 11, II, "f"):** quando o tratamento de dados de saúde é necessário para o cuidado realizado por profissionais de saúde vinculados.
- **Cumprimento de obrigação legal ou regulatória (art. 7º, II):** por exemplo, obrigações de farmacovigilância e guarda de registros.
- **Legítimo interesse (art. 7º, IX):** para segurança da informação, prevenção a fraudes e melhoria do serviço, sempre com teste de ponderação e sem prejuízo aos seus direitos.

SEÇÃO 08

Dados sensíveis de saúde

Boa parte dos dados que você registra na Aura são dados sensíveis. Por isso: (i) coletamos seu consentimento destacado para armazená-los; (ii) eles são confidenciais e só são compartilhados com a sua equipe de saúde quando você faz a vinculação; (iii) aplicamos controles de acesso e segregação lógica; e (iv) você pode, a qualquer momento, solicitar a exclusão da conta e dos dados associados, respeitadas as hipóteses legais de guarda.

SEÇÃO 09

Dados de menores e adolescentes

O tratamento de dados de crianças e adolescentes observa o art. 14 da LGPD e o princípio do melhor interesse. Como a Aura trata dados sensíveis de saúde, adotamos, por precaução, a regra de que a conta de qualquer paciente menor de 18 anos deve ser criada e gerida por pelo menos um dos pais ou pelo responsável legal, que representa o menor na plataforma e fornece o consentimento específico e em destaque exigido pelo art. 14, § 1º.

No momento do cadastro, coletamos a data de nascimento do titular e, ao aceitar esta Política e os Termos de Uso, o responsável declara agir nessa condição em nome do menor. A Aura pode solicitar a comprovação

dessa condição e, caso tome conhecimento de tratamento de dados de menor sem a devida autorização, adotará as medidas cabíveis, incluindo a eliminação dos dados.

Conforme entendimento da ANPD (Enunciado de 24/05/2023), o tratamento de dados de crianças e adolescentes pode se apoiar em outras bases legais dos arts. 7º e 11 da LGPD — como a tutela da saúde —, desde que prevaleça o melhor interesse do menor.

SEÇÃO 10

Compartilhamento e operadores (subprocessadores)

A Aura não vende seus dados pessoais. Compartilhamos dados apenas quando necessário para operar o serviço, com base legal adequada e sob obrigações contratuais de sigilo e segurança. As principais categorias são:

- **Sua equipe de saúde:** quando você vincula sua conta a uma clínica ou hospital, seus registros clínicos ficam acessíveis aos profissionais autorizados dessa instituição.
- **Operadores de infraestrutura e tecnologia:** fornecedores que hospedam e processam dados em nosso nome, nomeados abaixo.
- **Autoridades:** quando houver obrigação legal ou regulatória, ou para resguardar direitos.
- **Operações societárias:** em caso de reorganização ou venda de ativos, sempre preservando o nível de proteção desta Política; dados sensíveis não são compartilhados com potenciais compradores antes da efetivação, salvo estrita necessidade prevista em lei.

Fornecemos a cada operador apenas os dados necessários e exigimos, por contrato (acordo de tratamento de dados), padrão de proteção equivalente ao desta Política. Esta é a relação nominal dos operadores em uso, publicada e mantida atualizada:

Operador	Finalidade	Dados	Localização	Transferência internacional
Supabase	Banco de dados, autenticação, arquivos de exame e tarefas agendadas	Cadastro, dados de saúde e arquivos de exame	Brasil (São Paulo)	Não
Vercel	Hospedagem do painel institucional e do site	Metadados de acesso	Brasil (São Paulo)	Não
Cloudflare	Cópias de segurança cifradas (a Cloudflare não consegue abri-las); proteção de rede	Cópias cifradas com chave só da Aura	EUA	Sim (art. 33)
Railway	Execução da aplicação (processamento, sem armazenamento permanente)	Dados em trânsito	Exterior	Sim (art. 33)
Anthropic	Leitura automatizada de exames e conferência dos valores lidos (inteligência artificial)	Conteúdo do documento enviado	EUA	Sim (art. 33)

Operador	Finalidade	Dados	Localização	Transferência internacional
OpenAI	Reserva da leitura automatizada de exames, desligada: só volta a ser usada se a Anthropic ficar indisponível	Conteúdo do documento enviado, apenas enquanto estiver em uso	EUA	Sim (art. 33)
Expo	Distribuição do aplicativo e envio de notificações	Token de notificação e identificadores de dispositivo	EUA	Sim (art. 33)
Resend	Envio de e-mails: resumo diário à equipe, relatório semanal à gestão, convites e códigos de verificação do painel e contato pelo site	E-mail do destinatário; nos resumos à equipe, o código da paciente (nunca o nome), o título e a gravidade do alerta	EUA	Sim (art. 33)
Sentry	Monitoramento de falhas	Dados técnicos, com mascaramento de dados pessoais	EUA / União Europeia	Sim (art. 33)
PostHog	Estatísticas de uso (coleta desligada no app em 08/10/2026 e no painel da equipe em 11/10/2026; o histórico anterior foi removido em 11/10/2026, e o PostHog executa a exclusão dos eventos)	Nenhum dado novo. Do histórico anterior, em exclusão: identificador interno (sem nome nem e-mail), hospital e ações de uso; no app, também tipo de câncer, categoria e intensidade dos sintomas e registro de doses	EUA	Sim (art. 33)

SEÇÃO 11

Pesquisa clínica e científica

Podemos utilizar dados para pesquisa científica e clínica sobre saúde oncológica e a efetividade dos tratamentos, sempre de forma anonimizada. Antes de qualquer uso para pesquisa ou compartilhamento com parceiros de pesquisa, removemos ou substituímos as informações que possam identificá-lo, de modo que os dados deixem de permitir a sua identificação.

O uso de dados para pesquisa depende do seu consentimento específico, que você concede — e pode revogar a qualquer momento — nas preferências de privacidade do aplicativo, sem prejuízo do acesso às demais funcionalidades.

SEÇÃO 12

Comunicações de marketing

Utilizamos seu e-mail, telefone e notificações push para comunicações essenciais — autenticação, segurança e informações necessárias à prestação do serviço, como lembretes de medicação, consultas e exames. Essas comunicações são inerentes ao funcionamento do serviço.

Eventuais comunicações de marketing (novidades, conteúdos e informações sobre produtos e serviços da Aura) são enviadas apenas mediante o seu consentimento prévio (opt-in). Você pode revogar esse

consentimento a qualquer momento, nas configurações do aplicativo ou pelos canais de contato, sem que isso afete o acesso aos demais serviços e funcionalidades.

SEÇÃO 13

Transferência internacional

Mantemos no Brasil o banco de dados, os exames e documentos enviados e a hospedagem do painel e dos sites, tudo na região de São Paulo. Outros tratamentos ocorrem fora do país e você deve saber quais: a execução da aplicação, o envio de notificações, o envio de e-mails (os resumos à equipe identificam a paciente por um código, e não pelo nome), o monitoramento de falhas, as cópias de segurança, que saem cifradas com uma chave que só a Aura tem, e a leitura automatizada de documentos por inteligência artificial, que só acontece se você a autorizar e é processada nos Estados Unidos. As estatísticas de uso foram desligadas no aplicativo (08/10/2026) e no painel (11/10/2026); o histórico anterior foi removido em 11/10/2026, e o PostHog, que fica nos Estados Unidos, executa a exclusão dos eventos. A tabela de operadores acima indica a localização de cada um.

Nesses casos, a transferência internacional tem como referência os arts. 33 a 36 da LGPD e o Regulamento de Transferência Internacional de Dados (Resolução CD/ANPD nº 19/2024).

Para operadores localizados em países sem decisão de adequação da ANPD (como os Estados Unidos), os contratos de tratamento de dados que já conferimos — os da Anthropic, da OpenAI e da Cloudflare — usam as cláusulas-padrão contratuais da União Europeia e ainda não trazem as cláusulas-padrão aprovadas pela ANPD; a adoção destas está em análise. Para operadores localizados na União Europeia, aplica-se a decisão de adequação reconhecida pela ANPD.

SEÇÃO 14

Segurança da informação

Adotamos medidas técnicas e organizacionais compatíveis com a natureza sensível dos dados, incluindo: criptografia em trânsito (HTTPS); controle de acesso por papel e por instituição; segregação lógica de dados por meio de Row Level Security no banco de dados; registro de logs e trilhas de auditoria; e princípio do menor privilégio. Nenhum sistema é totalmente imune a incidentes; caso ocorra um incidente de segurança relevante, comunicaremos os titulares e a ANPD conforme a legislação.

Você também é corresponsável pela segurança: mantenha suas credenciais em sigilo e proteja o seu dispositivo.

SEÇÃO 15

Prazo de retenção

Mantemos seus dados pessoais apenas pelo tempo necessário às finalidades informadas, ao cumprimento de obrigações legais/regulatórias e ao exercício regular de direitos.

Os registros clínicos e de saúde (prontuário) são mantidos pelo prazo mínimo de 20 (vinte) anos, contado do último registro do paciente, nos termos da Lei nº 13.787/2018 (art. 6º) e da Resolução CFM nº 1.821/2007. No

caso de pacientes menores de idade, observa-se que o prazo prescricional não corre contra menores de 16 anos (art. 198, I, do Código Civil), o que pode estender, na prática, o período de guarda.

Os dados relacionados a eventos adversos (farmacovigilância) são mantidos enquanto necessário para fins de vigilância sanitária. Dados técnicos e de segurança (logs) são mantidos por período menor, conforme a necessidade de cada finalidade. Encerrada a necessidade, os dados são eliminados ou anonimizados.

SEÇÃO 16

Cookies e tecnologias semelhantes

Nossos aplicativos móveis (Android e iOS) não utilizam cookies; eventuais identificadores são armazenados localmente no seu dispositivo apenas para autenticação, funcionamento do aplicativo e, somente se você consentir, estatísticas de uso.

No painel clínico web e nos sites institucionais, utilizamos:

- **Cookies estritamente necessários:** indispensáveis para a autenticação, a manutenção da sessão e a segurança. Por serem essenciais ao funcionamento, não dependem de consentimento.
- **Analytics de produto (na área autenticada):** na área logada do painel clínico, utilizamos ferramentas de analytics de produto e de monitoramento de erros e desempenho para entender como os profissionais utilizam a ferramenta e aprimorá-la, com base no legítimo interesse. Não utilizamos cookies de publicidade nem compartilhamos esses dados com redes de anúncios.
- **Estatísticas do site institucional (somente com o seu consentimento):** o site pode carregar o Microsoft Clarity, que gera mapas de calor e gravações de navegação para entendermos onde o site confunde e grava os cookies _clck e _clsk. A Microsoft pode associar a visita a um identificador próprio (MUID), também usado por ela em publicidade; nós não usamos esses dados para anunciar. O Clarity só é carregado depois do aceite no aviso de cookies; sem escolha, é recusa, e recusar e aceitar custam o mesmo clique. Você pode mudar de ideia a qualquer momento em “Preferências de cookies”, no rodapé de qualquer página; ao recusar depois de ter aceitado, a ferramenta deixa de ser carregada e apagamos os cookies _clck e _clsk do nosso domínio. A escolha fica guardada só no seu navegador.

Os sites institucionais do Grupo Aura não empregam cookies de publicidade nem de rastreamento para marketing; as estatísticas do site descritas acima só são ativadas com o seu consentimento. Você pode gerenciar ou bloquear cookies nas configurações do seu navegador; a desativação dos cookies estritamente necessários pode comprometer funcionalidades essenciais do serviço.

SEÇÃO 17

Links de terceiros

Nossas plataformas podem conter links para sites ou serviços de terceiros que não controlamos. Esta Política não se aplica ao tratamento de dados realizado por esses terceiros; recomendamos a leitura das respectivas políticas de privacidade. A Aura não se responsabiliza pelo conteúdo nem pelas práticas de privacidade de sites de terceiros.

SEÇÃO 18

Seus direitos como titular

Nos termos da LGPD, você pode, a qualquer momento:

- confirmar a existência de tratamento e acessar seus dados;
- corrigir dados incompletos, inexatos ou desatualizados;
- solicitar anonimização, bloqueio ou eliminação de dados desnecessários ou tratados em desconformidade com a LGPD;
- solicitar a portabilidade dos dados a outro fornecedor;
- revogar o consentimento e solicitar a eliminação dos dados tratados com essa base;
- obter informação sobre com quem compartilhamos seus dados;
- peticionar perante a ANPD.

Para exercer qualquer direito, entre em contato com nosso Encarregado pelo e-mail privacidade@auraonco.com. Respondemos em até 15 (quinze) dias, nos termos do art. 19, II, da LGPD.

SEÇÃO 19

Farmacovigilância e eventos adversos

A Aura permite que você registre reações adversas a medicamentos. Os registros feitos pelo paciente entram como “a revisar” até serem confirmados por um profissional de saúde. Identificado um evento adverso, a Aura pode apoiar o seu encaminhamento às autoridades sanitárias pelos canais oficiais (por exemplo, o sistema VigiMed da Anvisa), conforme os protocolos de farmacovigilância aplicáveis.

Vale esclarecer que a obrigação formal de notificação de eventos adversos graves em prazo determinado (até 15 dias corridos, via VigiMed, conforme a RDC ANVISA nº 406/2020, com as alterações da RDC nº 967/2025) recai sobre os Detentores de Registro de Medicamento. O papel da Aura, salvo se e quando assumir essa condição, é registrar e facilitar o encaminhamento das notificações, sem substituir a responsabilidade regulatória do fabricante.

> **Importante — a Aura não realiza diagnóstico médico**
>
> A Aura é uma ferramenta que organiza e acompanha o cuidado. Seu conteúdo é informativo e não substitui a avaliação, o diagnóstico ou o tratamento de um profissional de saúde. Nunca desconsidere a orientação do seu médico nem deixe de procurar atendimento por causa de informações obtidas na plataforma. Em caso de dúvida sobre sua condição, consulte sempre um profissional de saúde qualificado.

SEÇÃO 20

Encarregado (DPO) e contato

Nosso Encarregado pelo Tratamento de Dados Pessoais é Matheus Celso Fachim dos Santos, que pode ser contatado pelo e-mail privacidade@auraonco.com ou pelo endereço Rua Paraná, nº 2781, Sala 2, Centro,

Cascavel/PR, CEP 85.812-011.

SEÇÃO 21

Alterações nesta Política

Podemos atualizar esta Política periodicamente. Em caso de alterações relevantes, notificaremos você pelo aplicativo ou pelo e-mail cadastrado com antecedência razoável. Manteremos as versões anteriores disponíveis mediante solicitação.

SEÇÃO 22

Legislação aplicável

Esta Política é regida pela legislação brasileira, em especial a LGPD, o Marco Civil da Internet e as normas da ANPD e da ANVISA aplicáveis. Fica eleito o foro do domicílio do titular para dirimir controvérsias, quando aplicável.

Dúvidas sobre os seus dados?

Fale com o nosso Encarregado (DPO), Matheus Celso Fachim dos Santos.

privacidade@auraonco.com

Respondemos em até 15 dias.

Aura Health Ltda. · CNPJ 67.652.854/0001-23 · Rua Paraná, 2781, Sala 2, Centro, Cascavel/PR, CEP 85.812-011
Política de Privacidade — Versão 1.9, vigente desde 18 de outubro de 2026.