Contrato de Operador — Acordo de Tratamento de Dados Pessoais (DPA) — Crommos Clinic

Este acordo é anexo dos Termos de Uso. A CONTROLADORA o aceita no cadastro, em caixa própria; a plataforma grava a versão deste acordo e a data do aceite.

Partes

- **CONTROLADORA:** a clínica ou o profissional que contrata o Crommos Clinic, identificada no cadastro da conta (razão social ou nome, CNPJ ou CPF e responsável).
- **OPERADORA:** Crommos, com sede em Teresópolis/RJ. Canal de comunicação: suporte@crommos.tech; encarregado: Elzo Junior (substituto: Roberto Azevedo).

1. Objeto

1.1. Este acordo regula o tratamento de dados pessoais que a OPERADORA realiza **em nome da CONTROLADORA** para prestar o software de gestão Crommos Clinic, nos termos dos arts. 37 a 40 da Lei 13.709/2018 (LGPD).

1.2. Não se aplica aos dados que a OPERADORA trata como controladora própria: cadastro da conta, dados de login e registros de acesso dos usuários da plataforma, cobrança da assinatura, suporte e segurança do serviço, descritos na Política de Privacidade.

2. Descrição do tratamento

Item	Descrição
Titulares	Pacientes (e responsáveis legais), profissionais e equipe da clínica, pagadores, tomadores de nota fiscal
Dados comuns	Identificação e contato (nome, CPF, nascimento, sexo, telefone, e-mail, endereço), convênio e carteirinha, dados financeiros, agenda, IP e registros de acesso e de aceite
Dados sensíveis (art. 11)	Dados de saúde: prontuário, evoluções, anamnese, alergias, exames e anexos, documentos clínicos (atestado, laudo, pedido de exame, receita), CID, teleconsulta, respostas de pesquisa de satisfação
Módulos	Agenda e agendamento online; Prontuário, documentos, assinatura digital e receita digital; Exames; Telemedicina (indisponível até a inscrição da OPERADORA no Conselho Regional de Medicina do Rio de Janeiro; Termos, cláusula 9.1); mensagens e pesquisa de satisfação; agenda no celular; Financeiro e recebimentos online; Fiscal; Convênio (TISS); Estoque; Múltiplas unidades; importação de dados; API pública e webhooks; exportação dos dados

Item	Descrição
Operações	Coleta, registro, armazenamento, organização, consulta, transmissão aos terceiros do Anexo I e aos integradores indicados pela CONTROLADORA (cláusula 4.7), cifra, cópia de segurança, exportação, anonimização e eliminação, sempre sob instrução da CONTROLADORA
Duração	Enquanto durar a assinatura, mais o período de devolução e eliminação (cláusula 10)

3. Instruções da CONTROLADORA

3.1. A OPERADORA trata os dados **somente** conforme este acordo, os Termos de Uso e as configurações feitas pela CONTROLADORA na plataforma (módulos contratados, canais de mensagem, acessos de cada pessoa, exigência de verificação em duas etapas, agendamento online, recebimentos online, autorização da Focus NFe, tokens da API e webhooks etc.), que valem como **instruções documentadas** (LGPD, art. 39).

3.2. A OPERADORA não usa os dados para finalidade própria, não os vende e não os usa para treinar modelos de inteligência artificial. Para cobrar a assinatura, usa só a contagem de pessoas marcadas em cada módulo e de teleconsultas concluídas (código do atendimento, sem dado do paciente).

3.3. A OPERADORA pode usar dados **anonimizados e agregados**, que não identificam titular nem clínica, para estatística e melhoria do produto.

3.4. A OPERADORA avisa a CONTROLADORA se entender que uma instrução viola a LGPD.

4. Responsabilidades da CONTROLADORA

4.1. **Base legal.** Definir a base legal de cada tratamento e obter o consentimento dos titulares quando ele for a base. A plataforma registra o consentimento por finalidade (com a versão do termo), o aceite do TCLE da teleconsulta e o aceite do aviso do agendamento online (data, hora, IP e versão). Bases indicadas pela OPERADORA para os recursos da plataforma, que a CONTROLADORA confirma no seu registro de operações:

- confirmação, lembrete, remarcação e cancelamento de consulta: execução do atendimento e tutela da saúde (art. 7º, V; art. 11, II, "f"), com aviso e opção de sair (SAIR no WhatsApp, link de descadastro no e-mail);
- comunicações e campanhas: consentimento (art. 7º, I);
- pesquisa de satisfação: legítimo interesse (art. 7º, IX), com teste de balanceamento registrado pela CONTROLADORA, aviso e opção de não receber;
- teleconsulta: tutela da saúde (art. 11, II, "f"), com o TCLE como exigência ética da Res. CFM 2.314/2022;
- faturamento de convênio (TISS): art. 11, II, "d" e "f", sem consentimento à parte;
- agenda no celular: legítimo interesse (art. 7º, IX), com o nome do paciente oculto por padrão.

4.2. **Transparência.** Informar os pacientes sobre o tratamento por um aviso de privacidade próprio, que inclua o agendamento online, as mensagens por e-mail e WhatsApp, a teleconsulta, a receita digital e a pesquisa de satisfação. A OPERADORA fornece um aviso-modelo (Anexo da Política de Privacidade), que a CONTROLADORA completa e adota.

4.3. **Operação.** Cadastrar dados corretos, inclusive o documento do paciente (sem ele, nem o CPF do responsável, o documento médico não é emitido) e o CRM, o RQE e os endereços que saem nos documentos médicos (Res. CFM 2.299/2021, art. 2º); definir quem da equipe acessa o quê; desativar usuários que saem; decidir se exige verificação em duas etapas (a OPERADORA recomenda fortemente exigi-la de quem acessa prontuário); guardar o prontuário pelo prazo legal (Lei 13.787/2018: no mínimo 20 anos).

4.4. **Integrações.**

- **Relações diretas da CONTROLADORA ou do profissional:** a conta no gateway de pagamento que a CONTROLADORA escolher e conectar para os recebimentos online (AbacatePay, Asaas, Efí ou Stripe; no máximo um ativo), contratada direto por ela — o gateway não é suboperador da OPERADORA, que só usa as credenciais da CONTROLADORA para criar e conferir as cobranças e não recebe nem guarda valores —, o certificado A1 da clínica (NFS-e) e o certificado ICP-Brasil que o médico contratar por conta própria com um prestador de serviço de certificação (PSC), que atua como controlador próprio.
- **Soluti (BirdID Pro):** a OPERADORA contrata a Soluti para a assinatura digital ICP-Brasil dos documentos médicos, com um certificado em nuvem que a Soluti emite para o médico e que só assina dentro do Crommos Clinic. O motor de assinatura roda na infraestrutura da OPERADORA, no Brasil: o documento não sai dela. À Soluti vão o CPF do médico e o código do aplicativo BirdID, para abrir a sessão de assinatura, e só o código (hash) de cada documento. Na sessão, na assinatura e na licença, a Soluti é suboperadora da OPERADORA; na emissão e na gestão do certificado do médico, é autoridade certificadora da ICP-Brasil e controladora. A receita não é assinada pela Soluti: segue na Memed.
- **Focus NFe:** em município com emissor próprio, o administrador da CONTROLADORA dá autorização expressa na plataforma (versão do texto, quem e quando ficam registrados) para a OPERADORA cadastrá-la na Focus NFe, suboperadora da OPERADORA, com o certificado A1 e a senha, e emitir por ela. Retirar a autorização ou voltar ao emissor nacional faz a OPERADORA remover na hora o cadastro e o certificado na Focus NFe; no término da assinatura, a remoção é feita no início do modo leitura. O contrato da OPERADORA com a Focus NFe exige dados no Brasil, sigilo e eliminação do certificado A1 ao revogar.
- **Memed (receita digital):** a OPERADORA cadastra o médico na Memed e envia os dados do médico e do paciente necessários, inclusive as alergias. No cadastro do prescritor e na emissão, a Memed é suboperadora da OPERADORA; no que faz por conta própria, como o envio da receita ao paciente, é controladora.
- **Integradores por API:** ver a cláusula 4.7.

4.5. **Importação.** A CONTROLADORA garante que tem base legal para importar dados de outro sistema e que o arquivo enviado se limita ao necessário.

4.6. **Agenda no celular.** O link de calendário é pessoal do profissional e, por padrão, não mostra o nome do paciente. A CONTROLADORA orienta a equipe a não compartilhar o link e a só mostrar o nome abreviado quando adequado.

4.7. **API pública e webhooks.** O administrador da CONTROLADORA pode criar tokens de acesso à API e cadastrar webhooks para ligar o Crommos Clinic a outro sistema (site, chatbot, BI etc.).

- **Quem é o integrador.** A empresa ou pessoa que recebe o token (o "integrador") é escolhida e contratada pela CONTROLADORA. Ela **não é suboperadora da OPERADORA**: trata os dados em nome da CONTROLADORA ou como controladora própria, conforme o contrato entre as duas. A

CONTROLADORA responde pela escolha, pelo contrato com o integrador (art. 39) e pelo que ele fizer com os dados recebidos. A OPERADORA não responde pelo tratamento feito pelo integrador depois da entrega.

- **Instrução.** Criar um token, escolher os escopos e cadastrar um webhook são instruções da CONTROLADORA para a OPERADORA entregar ao integrador os dados daqueles escopos. Ao criar o token, o administrador declara, numa caixa própria, que a CONTROLADORA tem contrato com quem vai usar o token e responde pelo uso dos dados; sem essa declaração, o token não é criado.
- **Mínimo necessário (art. 6º, III).** A CONTROLADORA dá ao integrador só os escopos de que ele precisa e a menor validade possível. A API não entrega prontuário, exames, documentos clínicos, endereço nem responsável, e não lista o cadastro inteiro: a busca de pacientes exige ao menos 3 caracteres. A observação do agendamento entra pela API, mas não volta nas respostas. A agenda ainda pode revelar dado de saúde (especialidade, procedimento e motivo de cancelamento): a CONTROLADORA não escreve informação clínica nesses campos e trata o integrador como quem recebe dado sensível.
- **Webhooks.** O aviso leva só o tipo do evento e códigos (ids), sem dado do paciente; o integrador busca o restante com o token. O endereço precisa ser HTTPS e público.
- **Transferência internacional.** Se o integrador tratar os dados fora do Brasil, a transferência é da CONTROLADORA, que garante a hipótese do art. 33.
- **Transparência e direitos.** A CONTROLADORA informa os pacientes sobre o integrador no seu aviso de privacidade e, quando corrigir ou anonimizar um cadastro, avisa o integrador (art. 18, § 6º).
- **Revogação.** A CONTROLADORA revoga o token e remove o webhook quando o integrador deixar de prestar o serviço ou se houver suspeita de vazamento. O token vence na validade escolhida (até 365 dias) e deixa de valer na hora para o módulo retirado da assinatura. A OPERADORA pode **suspender** um token ou webhook diante de vazamento ou uso anormal e avisa a CONTROLADORA no mesmo dia.
- **Registro.** A OPERADORA registra na trilha de auditoria as gravações feitas pela API e as leituras do cadastro de pacientes e da agenda (com os códigos dos registros e dos pacientes lidos), com o token como autor, e guarda o último uso e o IP de cada token. Ao criar o token, a trilha guarda a declaração do administrador, com a cláusula e a versão dos Termos de Uso. Criar e revogar token avisa todos os administradores.
- **Término.** No modo leitura, o token continua lendo até vencer ou ser revogado, e a CONTROLADORA pode revogá-lo e remover o webhook a qualquer momento; na eliminação (cláusula 10), tokens e webhooks são apagados com os demais dados.

5. Obrigações da OPERADORA

5.1. **Confidencialidade.** Acesso aos dados só por pessoas autorizadas, sob dever de sigilo, e só quando necessário (suporte a pedido da CONTROLADORA, incidente, obrigação legal).

5.2. **Segurança (art. 46).** Medidas técnicas em vigor:

- isolamento por clínica no banco de dados;
- cifra AES-256-GCM de CPF, e-mail, telefone, conteúdo clínico, anexos, chaves de integração e certificados, com rotação de chave que recifra todos os dados cifrados;
- conexão segura (TLS); senhas guardadas só como resumo criptográfico; controle de acesso por papel, por módulo e por vínculo do profissional com o paciente;

- **verificação em duas etapas** (aplicativo autenticador e códigos de recuperação), que a CONTROLADORA pode exigir de administradores e de quem acessa prontuário;
- **registros de acesso** (login, logout, senha, verificação em duas etapas) com IP, navegador, data e hora (Marco Civil, art. 15);
- **trilha de auditoria imutável** (leitura de prontuário, leitura do cadastro de pacientes e da agenda pela API, exportação, aceites, importação, DMED, autorização da Focus NFe, eliminação por prazo e no término), com IP e navegador;
- **exportação completa** só pelo administrador, com aviso na tela de que o arquivo tem dado de saúde e aviso aos demais administradores a cada exportação;
- **alerta de leitura anômala** de prontuário ao administrador e ao gestor da clínica;
- **eliminação automática** diária do que venceu, nos prazos da Política de Privacidade;
- cópia de segurança cifrada fora do servidor, com teste de restauração;
- links públicos (teleconsulta, pesquisa, agendamento, validação de documento, agenda no celular) com código imprevisível, validade e limite de acessos; o QR do documento assinado mostra quem assinou e, só com assinatura ICP-Brasil, entrega o PDF assinado, por 1 ano, com cada consulta na trilha de auditoria; link de pagamento sem dado nenhum, válido por 7 dias; QR PIX de 15 minutos;
- mensagens e pagamentos sem dado clínico; teleconsulta sem gravação e **sem chat**;
- **transcrição local da consulta**: o áudio é transcrito no navegador do médico, **não sai do computador nem é guardado**; a trilha registra só que o médico confirmou o aviso ao paciente;
- **assinatura pelo BirdID Pro**: sessão de no máximo 12 horas, aberta pelo código do aplicativo do médico, guardada cifrada e usada só pelo próprio médico logado; termina no botão "Encerrar sessão" e no logout; cada documento exige um clique em Assinar, sem assinatura em lote; abertura e encerramento da sessão na trilha de auditoria;
- credenciais das integrações guardadas fora do banco de dados ou cifradas;
- **API pública:** token guardado só como resumo criptográfico, mostrado uma vez, com validade obrigatória, escopo por módulo, no máximo 3 válidos por clínica, só HTTPS e limite de requisições; segredo do webhook cifrado; webhook só para endereço público, sem seguir redirecionamento;
- sessão com renovação por cookie protegido.

5.3. **Direitos dos titulares (arts. 18 a 22).** A OPERADORA oferece na plataforma a **exportação completa**, a **correção** e a **anonimização do cadastro** do paciente, também no modo leitura, qualquer que seja o motivo dele, e apoia a CONTROLADORA nos pedidos que ela não consiga atender sozinha, em até **5 dias úteis**. Pedido que chegar diretamente à OPERADORA é repassado à CONTROLADORA em até **2 dias úteis**, sem resposta de mérito ao titular.

5.4. **Depois do término.** Se o titular procurar a OPERADORA após o término da assinatura, a OPERADORA o orienta a procurar a CONTROLADORA e, durante os 90 dias de modo leitura, apoia a CONTROLADORA a atender o pedido.

5.5. **Apoio a relatório de impacto e à ANPD.** Fornecer as informações necessárias ao relatório de impacto (art. 38) e a fiscalizações.

6. Incidentes de segurança

6.1. A OPERADORA comunica à CONTROLADORA incidente de segurança confirmado com os dados dela em até **24 horas** da ciência, mesmo antes de concluir a apuração, com o que já souber: data da ocorrência e da ciência, descrição e causa provável, natureza e categoria dos dados (e se estavam cifrados), número de titulares afetados (separando crianças, adolescentes e idosos, quando possível) e total de titulares da atividade afetada, medidas de segurança anteriores e posteriores, riscos, medidas tomadas e previstas e contato da OPERADORA. Completa as informações à medida que apurar. São os dados de que a CONTROLADORA precisa para a comunicação (Res. CD/ANPD 15/2024, arts. 6º, § 2º, e 9º).

6.2. A comunicação à ANPD e aos titulares (art. 48) é da CONTROLADORA, com o apoio da OPERADORA, em **3 dias úteis** contados de quando ela soube que o incidente afetou dados pessoais (Res. CD/ANPD 15/2024, arts. 6º e 9º). A informação à ANPD pode ser complementada em até 20 dias úteis.

6.3. Quando o mesmo incidente atingir várias clínicas, a OPERADORA pode comunicar a ANPD **por mandato** das clínicas que autorizarem, sem tirar delas o dever legal de comunicar. A autorização é uma procuração com poderes de representação perante a ANPD, que acompanha a comunicação dentro do prazo (Res. CD/ANPD 15/2024, art. 6º, §§ 5º e 6º).

6.4. A OPERADORA mantém o seu próprio registro dos incidentes com dados da CONTROLADORA, inclusive os não comunicados, por 5 anos, e entrega cópia da parte que lhe diz respeito quando pedida, para o registro da CONTROLADORA (Res. CD/ANPD 15/2024, art. 10).

6.5. Incidente no sistema do integrador indicado pela CONTROLADORA (cláusula 4.7) é tratado entre a CONTROLADORA e o integrador. A OPERADORA apoia com a revogação do token e os registros que tiver.

7. Suboperadores

7.1. A CONTROLADORA autoriza os suboperadores do Anexo I — Suboperadores.

7.2. A OPERADORA avisa com **30 dias** de antecedência a inclusão ou troca de suboperador, por e-mail ao administrador da conta e por aviso na plataforma. A CONTROLADORA pode se opor de forma fundamentada; sem acordo, pode encerrar a assinatura sem multa. Se a troca for urgente, por segurança ou porque o suboperador deixou de prestar o serviço, a OPERADORA avisa assim que trocar e a CONTROLADORA mantém o mesmo direito de objeção.

7.3. A OPERADORA exige de cada suboperador obrigações de proteção equivalentes às deste acordo e responde perante a CONTROLADORA pelos atos dele (art. 42, § 1º, I).

8. Transferência internacional

8.1. A regra é tratar os dados **no Brasil**. Há transferência de metadados e de dados de contato para os EUA com **Daily** (teleconsulta, só depois de liberada a Telemedicina), **Resend** (e-mail) e **Meta** (WhatsApp), conforme o Anexo I, sem conteúdo clínico.

8.2. Essas transferências se apoiam nas **cláusulas-padrão contratuais da ANPD** (LGPD, art. 33, II, "b", e Res. CD/ANPD 19/2024), adotadas na íntegra e sem alteração nos contratos da OPERADORA com esses suboperadores (Res. CD/ANPD 19/2024, art. 16), na Opção B do Anexo II (transferência entre operadores), com a CONTROLADORA como "Terceiro Controlador" e este acordo como contrato coligado. Por este

acordo, a CONTROLADORA **instrui por escrito** a OPERADORA a fazer essas transferências, nos limites do Anexo I. Se um desses suboperadores não aceitar as cláusulas, a OPERADORA o troca por outro, com o aviso da cláusula 7.2.

8.3. A CONTROLADORA pode desligar os canais de e-mail e WhatsApp e não contratar a Telemedicina.

8.4. Gateway de pagamento com tratamento fora do Brasil (ex.: Stripe) é escolha e contrato da CONTROLADORA, sob as garantias que o gateway oferece a ela. A OPERADORA não envia a ele dado pessoal do paciente (só valor, descrição genérica e referência interna); os dados do pagamento o paciente informa direto ao gateway, o que é coleta do próprio gateway, não transferência da OPERADORA (Res. CD/ANPD 19/2024, art. 6º).

8.5. Cabe à CONTROLADORA, como controladora, informar os pacientes sobre as transferências internacionais e entregar a íntegra das cláusulas a quem pedir, em 15 dias (Res. CD/ANPD 19/2024, art. 17). A OPERADORA fornece o texto do aviso-modelo (Anexo da Política de Privacidade) e cópia das cláusulas quando a CONTROLADORA pedir.

9. Auditoria

9.1. A CONTROLADORA pode pedir, uma vez por ano ou após incidente, evidências de conformidade (relatórios, políticas, respostas a questionário), que a OPERADORA entrega em até 30 dias.

9.2. Auditoria presencial ou por auditor independente: com aviso de 30 dias, em horário comercial, uma vez por ano (salvo após incidente ou por determinação da ANPD), sob compromisso de confidencialidade, sem acesso a dados de outras clínicas e com os custos a cargo da CONTROLADORA.

10. Término: devolução e eliminação

10.1. Após o término, a conta fica **90 dias em modo leitura** para a CONTROLADORA exportar todos os dados em formato legível. O término é o dia seguinte ao último dia de uso, na assinatura cancelada, o fim da avaliação não contratada ou, no atraso de pagamento, o dia em que a conta completa 60 dias seguidos em modo leitura (Termos de Uso, cláusula 4.7); pagar antes disso reativa a conta. A OPERADORA avisa os administradores da CONTROLADORA por e-mail 30 e 7 dias antes da eliminação (sem administrador, o aviso vai ao e-mail de cobrança); aviso atrasado adia a eliminação para manter essa antecedência. Contratar ou reativar a assinatura antes da data cancela a eliminação. No término, a OPERADORA remove o cadastro e o certificado A1 da Focus NFe.

10.2. Depois disso, a OPERADORA elimina os dados e os arquivos da CONTROLADORA, inclusive tokens e webhooks, retira os acessos das pessoas à conta e elimina os dados das cópias de segurança em até 30 dias, **exceto** o que a lei a obrigue a guardar. Ficam a razão social e o CNPJ da CONTROLADORA, os dados de cobrança e fiscais da assinatura (5 anos) e a trilha de auditoria, sem o conteúdo dos registros, pelo prazo da Política de Privacidade (5 anos; IP e navegador, 1 ano), como prova do tratamento realizado (LGPD, art. 6º, X). O login de quem só tinha acesso à conta da CONTROLADORA é anonimizado na plataforma, conforme a Política de Privacidade.

10.3. A guarda do prontuário por no mínimo 20 anos (Lei 13.787/2018) é da CONTROLADORA, que deve exportá-lo e guardá-lo antes do fim do modo leitura. A OPERADORA não guarda prontuário depois desse prazo.

11. Responsabilidade

11.1. Cada parte responde pelos danos que causar por violar a LGPD (arts. 42 a 45).

11.2. A responsabilidade total da OPERADORA por este acordo e pelos Termos de Uso fica limitada ao valor pago pela CONTROLADORA nos 12 meses anteriores ao fato, exceto em caso de dolo ou culpa grave e nas hipóteses em que a lei não permite limitar a responsabilidade.

11.3. Nenhuma das partes é obrigada a contratar seguro específico para este serviço.

12. Disposições finais

Este acordo prevalece sobre os Termos de Uso no que tratar de dados pessoais. Lei brasileira. Fica eleito o foro da comarca de Teresópolis/RJ, salvo quando a CONTROLADORA for consumidora, caso em que vale o foro do domicílio dela (Código de Defesa do Consumidor).

Anexo I: Suboperadores.