Suboperadores e terceiros — Crommos Clinic (Anexo I do Contrato de Operador)

Anexo do Contrato de Operador (DPA) entre a clínica e a Crommos, com sede em Teresópolis/RJ.

Papéis

- **Clínica** (cliente): **controladora** dos dados dos pacientes, da equipe e da operação (LGPD, art. 5º, VI).
- **Crommos: operadora** (art. 5º, VII, e art. 39). Também é **controladora** dos dados cadastrais e de cobrança da própria clínica cliente (conta, usuários da plataforma, assinatura).
- **Suboperador:** terceiro contratado **pela Crommos** que trata dado pessoal da clínica para prestar o serviço.
- **Fornecedor da clínica ou do médico:** terceiro com quem a **clínica ou o profissional** tem relação própria (conta, certificado, obrigação fiscal) e que trata os dados como controlador próprio. A Crommos só faz a integração técnica.
- **Integrador indicado pela clínica:** quem recebe da clínica um token da API pública (site, chatbot, BI). A clínica escolhe, contrata e responde por ele (DPA, cláusula 4.7). Não é suboperador da Crommos.

Resumo

#	Terceiro	Papel	Local de processamento
1	Hostinger — servidor virtual (VPS)	Suboperador	Brasil
2	Provedor de armazenamento de arquivos e cópias de segurança	Suboperador	Brasil
3	Daily (Daily.co, Inc., EUA)	Suboperador (só depois de liberada a Telemedicina)	Mídia em São Paulo; conta, registros e metadados nos **EUA**
4	Resend (Resend, Inc., EUA)	Suboperador	Envio a partir de São Paulo; conta, registros e metadados nos **EUA**
5	Meta — WhatsApp Business Platform	Suboperador	Data centers da Meta (EUA e outros países)
6	Memed (Memed S.A., Brasil)	Suboperadora no cadastro do prescritor e na emissão; controladora no que faz por conta própria	Brasil (nuvem em São Paulo)

#	Terceiro	Papel	Local de processamento
7	Soluti — BirdID Pro (assinatura digital, Brasil)	Suboperadora na sessão, na assinatura e na licença; controladora como autoridade certificadora na emissão do certificado	Brasil (motor de assinatura no servidor da Crommos)
8	Outros prestadores de assinatura digital em nuvem (PSCs), com o certificado próprio do médico	Fornecedores do médico (controladores próprios)	Brasil (PSCs credenciados pelo ITI)
9	Gateway de pagamento da clínica (AbacatePay, Asaas, Efí ou Stripe) — recebimentos online	Fornecedor da clínica	Brasil (AbacatePay, Asaas, Efí); Stripe também fora do Brasil
10	AbacatePay — assinatura da plataforma	Operador da Crommos (como controladora)	Brasil
11	Receita Federal — Emissor Nacional da NFS-e	Autoridade pública (destinatária legal)	Brasil
12	Focus NFe	Suboperador	Brasil
13	Operadoras de plano de saúde (TISS)	Destinatárias e controladoras próprias	Brasil
14	Integradores da API pública (site, chatbot, BI da clínica)	Indicados pela clínica (operadores ou controladores dela)	Onde o integrador estiver; escolha da clínica

Detalhe por terceiro

1. Hostinger — servidor virtual

- **Finalidade:** hospedar a aplicação, o banco de dados e o processamento de todos os módulos.
- **Dados:** todos os dados da clínica; campos sensíveis cifrados com AES-256-GCM (CPF, e-mail, telefone, conteúdo clínico, anexos), com a chave fora do banco de dados.
- **Base legal:** a de cada tratamento (é infraestrutura).
- **Contrato:** servidor em data center no Brasil (região escolhida ao criar o servidor), com obrigações de proteção equivalentes às do DPA. A Hostinger é empresa estrangeira; os dados ficam no servidor no Brasil.

2. Armazenamento de arquivos e cópias de segurança

- **Finalidade:** anexos (exames, documentos assinados) e cópias de segurança do banco de dados e dos anexos, fora do servidor.
- **Dados:** arquivos clínicos e cópia do banco de dados, **cifrados antes de sair da aplicação** (anexos com AES-256-GCM; a cópia do banco e o pacote de anexos, também inteiros, com chave pública cuja chave privada fica fora do servidor); o provedor não tem a chave. Cópias guardadas por 30 dias. O espelho dos anexos acompanha a origem: o arquivo apagado na aplicação (clínica eliminada, anonimização) vira versão antiga no destino e é apagado em 28 dias pela regra de ciclo de vida do bucket, que precisa ter versionamento ligado.
- **Base legal:** a de cada tratamento; guarda do prontuário: art. 11, II, "a" (Lei 13.787/2018).

- **Contrato:** provedor com armazenamento em região no Brasil (provedor sem região no Brasil não serve), com obrigações de proteção equivalentes às do DPA. O nome do provedor entra nesta lista antes do início do serviço; uma troca posterior segue o aviso de 30 dias.

3. Daily

- **Situação:** não recebe dado enquanto a Telemedicina estiver indisponível (Termos, cláusula 9.1). O contrato com as cláusulas-padrão da ANPD é assinado antes da liberação.
- **Finalidade:** teleconsulta: vídeo e áudio em tempo real, **sem gravação e sem chat**.
- **Dados:** imagem e som em trânsito; nome exibido ("Paciente" e o nome do médico); IP e metadados técnicos da conexão. Sala com nome aleatório, sem dado do paciente. Sala de teste de câmera: só o médico, nome "Teste de câmera", 10 minutos, nada gravado.
- **Base legal:** art. 11, II, "f" (tutela da saúde).
- **Transferência internacional:** cláusulas-padrão contratuais da ANPD (Res. CD/ANPD 19/2024).
- **Retenção:** registros técnicos da chamada pelo prazo de retenção do plano contratado, apagados automaticamente; no fim do contrato, devolução ou eliminação (DPA do Daily, seção 2.4 e Anexo C).
- **Contrato:** acordo de tratamento de dados do Daily, com as cláusulas-padrão da ANPD.

4. Resend

- **Finalidade:** e-mails de confirmação, lembrete, remarcação, cancelamento, pesquisa de satisfação e link de pagamento; e-mails da equipe (convite, senha, aviso de verificação em duas etapas desligada).
- **Dados:** nome e e-mail do destinatário, nome da clínica, data e hora, profissional e local da consulta, links. **Sem dado clínico.**
- **Base legal:** confirmação e lembretes: art. 7º, V, e art. 11, II, "f" (execução do atendimento e tutela da saúde), com opção de sair; pesquisa de satisfação: art. 7º, IX (legítimo interesse da clínica), com opção de sair; e-mails da equipe: art. 7º, V.
- **Transferência internacional:** cláusulas-padrão contratuais da ANPD.
- **Retenção:** e-mails e registros de envio por 30 dias (retenção do plano); no fim do contrato, eliminação em até 90 dias (DPA da Resend, Anexo A).
- **Contrato:** acordo de tratamento de dados da Resend, com as cláusulas-padrão da ANPD.

5. Meta (WhatsApp Business Platform)

- **Finalidade:** lembrete, remarcação, cancelamento e link de pagamento por WhatsApp; respostas do paciente (confirmar, cancelar, sair).
- **Dados:** telefone, primeiro nome, clínica, data e hora, profissional, local, links, texto da resposta. **Sem dado clínico.** A Meta guarda o conteúdo por até 30 dias.
- **Conta:** a conta na Meta é da Crommos; as mensagens saem com o nome da clínica. O custo está incluído na assinatura (franquia do nível da Agenda; excedente de R$ 0,05 por mensagem).
- **Base legal:** como o item 4.
- **Transferência internacional:** cláusulas-padrão contratuais da ANPD.
- **Contrato:** termos de tratamento de dados da Meta para a plataforma de WhatsApp Business.

6. Memed (receita digital)

- **Finalidade:** emissão de receita, inclusive de controle especial, no painel da Memed dentro da tela de atendimento ("Nova receita"; "Renovar" para uso contínuo). A tela chama o serviço de "receita digital"; a Memed é nomeada nesta lista e na Política de Privacidade.
- **Como funciona:** a Crommos contrata a Memed, cadastra o médico nela e obtém o acesso dele; o painel da Memed roda no navegador do médico.
- **Dados enviados:**
  - **prescritor:** nome, CPF, nascimento, CRM/UF, e-mail, especialidade e cidade;
  - **paciente:** nome, nome social, sexo, CPF, nascimento, telefone, e-mail e as **alergias** do prontuário (convertidas em princípios ativos da tabela da Memed);
  - **local:** CNES e endereço, só quando a clínica tem CNES;
  - **conteúdo da receita** (dado de saúde), digitado no painel da Memed ou pré-preenchido ao renovar.
- **Base legal:** art. 11, II, "f" (tutela da saúde) e "a" (obrigação regulatória: receituário de controle especial).
- **Papel:** arranjo misto. No cadastro do prescritor e na emissão, a Memed é suboperadora da Crommos, com contrato e obrigações equivalentes às do DPA. No que faz por conta própria, como o envio da receita ao paciente, é controladora, sob a política dela.

7. Soluti — BirdID Pro (assinatura digital)

- **Situação:** contrato em negociação. Até ele ser assinado, o BirdID Pro roda só em homologação, com dados fictícios, e nenhum dado real vai à Soluti. Antes do primeiro dado real, o contrato precisa prever: tratamento só por instrução da Crommos; dados no Brasil; eliminação ao fim do contrato; lista de subcontratados, com aviso de troca; acesso da equipe técnica da Soluti ao sistema só na homologação, sem dado real; aviso de incidente à Crommos em até 24 horas.
- **Finalidade:** assinatura digital ICP-Brasil de atestado, laudo, encaminhamento, pedido de exame e evolução, com o certificado em nuvem que a Crommos oferece ao médico. A receita não é assinada por aqui: segue na Memed (item 6).
- **Como funciona:** a Crommos contrata a Soluti e paga a licença por médico ativo. O médico recebe da Soluti, sem custo, um certificado ICP-Brasil em nuvem (e-CPF A3) que só assina dentro do Crommos Clinic. O motor de assinatura da Soluti roda no servidor da Crommos no Brasil (item 1), sem acesso pela internet: o PDF é assinado ali e não vai à Soluti. O PDF assinado fica no motor por até 1 hora e é guardado cifrado no Crommos, como os anexos.
- **Sessão de assinatura:** o médico digita o código do aplicativo BirdID e abre uma sessão de até 12 horas. O token da sessão fica cifrado no cadastro do profissional e só o próprio médico, logado, o usa. Cada documento exige um clique em **Assinar**, sem assinatura em lote. A sessão termina no botão **Encerrar sessão** e no logout. A abertura e o encerramento ficam na trilha de auditoria.
- **Dados enviados à Soluti:** para abrir a sessão, o CPF do médico e o código do aplicativo; para assinar, **só o código (hash)** de cada documento, com o token da sessão; para a licença, o uso por médico. **Nome, documento e conteúdo clínico do paciente não saem da Crommos.** O CRM, a UF do CRM e o tipo do documento ficam dentro do PDF assinado, como atributos da ICP-Brasil.
- **Base legal:** art. 7º, II e V; art. 11, II, "a" (Lei 14.063/2020; Res. CFM 2.299/2021).
- **Papel:** arranjo misto. Na sessão, na assinatura e na licença, a Soluti é suboperadora da Crommos, com contrato e obrigações equivalentes às do DPA. Na emissão, na renovação e na revogação do

certificado do médico, inclusive na confirmação da identidade dele, é autoridade certificadora da ICP-Brasil e controladora, sob as regras da ICP-Brasil (MP 2.200-2/2001, art. 6º).

- **Local:** Brasil. O motor de assinatura fica no servidor da Crommos; o local dos dados na Soluti entra no contrato. Em homologação, o motor hospedado pela Soluti recebe só dados fictícios.
- **Contrato:** licença do BirdID Pro com cláusulas de proteção de dados (ver Situação).

8. Outros prestadores de assinatura digital em nuvem — certificado próprio do médico (BirdID, VIDaaS, SerproID, SafeID, RemoteID)

- **Quando:** o médico usa o certificado ICP-Brasil que ele mesmo contratou, em vez do BirdID Pro.
- **Finalidade:** assinatura digital ICP-Brasil de atestado, laudo, encaminhamento, pedido de exame e evolução.
- **Dados: só o código (hash SHA-256)** do documento (o documento não sai da Crommos) e o identificador do certificado do médico.
- **Base legal:** art. 7º, II e V; art. 11, II, "a" (Lei 14.063/2020; Res. CFM 2.299/2021).
- **Papel:** fornecedor contratado pelo próprio médico, que trata os dados como controlador próprio.

9. Gateway de pagamento da clínica — recebimentos online

- **Quem:** o gateway que a clínica escolher e conectar (AbacatePay, Asaas, Efí ou Stripe), no máximo um ativo por vez.
- **Finalidade:** link ou QR de pagamento PIX e cartão; sinal ao agendar; baixa automática.
- **Dados enviados pela Crommos:** valor, descrição genérica ("Pagamento — clínica", "Sinal — consulta de" e o dia) e referência interna. **Sem nome, CPF ou dado clínico.** Os dados do pagador são digitados pelo paciente direto na página do gateway. O link da Crommos vale 7 dias.
- **Base legal:** art. 7º, V (contrato entre clínica e paciente).
- **Papel: fornecedor da clínica**, não suboperador da Crommos. A clínica contrata o gateway, conecta a própria conta e aceita os termos dele; o dinheiro vai direto para essa conta. A Crommos só faz a integração técnica com as credenciais da clínica (cifradas): criar a cobrança, consultar o pagamento e, na Efí, cadastrar o webhook.
- **Local:** AbacatePay, Asaas e Efí no Brasil. A **Stripe** pode tratar os dados do pagador fora do Brasil, sob as garantias que ela dá à clínica; a Crommos não envia dado pessoal do paciente a ela.

10. AbacatePay — assinatura da plataforma

- **Finalidade:** cobrança recorrente da assinatura Crommos.
- **Dados:** responsável e CNPJ da clínica e dados do pagamento. Não envolve dado de paciente.
- **Base legal:** art. 7º, V.

11. Receita Federal — Emissor Nacional da NFS-e

- **Finalidade:** emissão e cancelamento de NFS-e.
- **Dados:** tomador (nome, CPF/CNPJ e endereço do paciente, do responsável ou da operadora); valor e código do serviço. A descrição é um texto fixo da configuração fiscal (padrão "Consulta médica"), **sem diagnóstico**.
- **Base legal:** art. 7º, II, e art. 11, II, "a" (obrigação tributária).

12. Focus NFe

- **Finalidade:** NFS-e em município com emissor próprio (ex.: São Paulo capital), só quando o administrador da clínica dá a autorização expressa.
- **Dados:** clínica (razão social, CNPJ, inscrição municipal, regime, e-mail, telefone, endereço e o **certificado A1 com a senha**); nota (tomador, valor, serviço e descrição). A chave de acesso de cada clínica fica cifrada na Crommos. Sem dado clínico.
- **Autorização:** dada ou retirada só pelo administrador da clínica; o sistema grava quem, quando e a versão do texto e registra na trilha de auditoria. Sem ela, nada vai à Focus NFe. Retirar a autorização ou voltar ao emissor nacional remove na hora a empresa e o certificado na Focus NFe, inclusive no modo leitura. No término da assinatura, a remoção é automática, no início do modo leitura.
- **Base legal:** art. 7°, II (obrigação tributária); envio do A1 por instrução da clínica (DPA, cláusula 4.4).
- **Contrato:** dados no Brasil, sigilo e eliminação do certificado A1 e do cadastro ao revogar.

13. Operadoras de plano de saúde (TISS)

- **Finalidade:** faturamento de convênio.
- **Dados:** identificação, carteirinha, procedimentos e, se exigido pela operadora, CID.
- **Base legal:** art. 11, II, "d" (exercício regular de direitos em contrato) e "f" (tutela da saúde), sem consentimento à parte.

14. Integradores da API pública

- **Quem:** o sistema que a clínica liga ao Crommos Clinic (site, chatbot de WhatsApp ou Instagram, BI), com o token que o administrador da clínica cria em Configurações › API.
- **Finalidade:** a que a clínica definir no contrato com o integrador (em geral, marcar consultas e manter o cadastro).
- **Dados:** só os escopos que a clínica escolher: agenda (horários, profissional, unidade, especialidade, procedimento, situação, motivo de cancelamento; a observação entra, mas não volta nas respostas), cadastro do paciente (nome, nome social, CPF, nascimento, sexo, e-mail, telefone, convênio e carteirinha), sempre por busca de ao menos 3 caracteres, e lançamentos do financeiro. **Sem prontuário, exames, documentos clínicos, endereço nem responsável.** A agenda pode revelar dado de saúde (especialidade, procedimento). Os webhooks levam só o tipo do evento e códigos (ids).
- **Base legal:** a da clínica para cada uso (em geral, art. 7°, V, e art. 11, II, "f").
- **Papel: indicado pela clínica**, não suboperador da Crommos (DPA, cláusula 4.7). A clínica contrata o integrador, responde por ele e, se ele tratar os dados fora do Brasil, pela transferência (art. 33); o administrador declara esse contrato ao criar o token. A Crommos entrega os dados só com token válido, registra as gravações e as leituras do cadastro de pacientes e da agenda com o token como autor e pode suspender o token diante de vazamento.

Sem terceiro ou sem dado de paciente

Feitos na própria Crommos: agendamento online, pesquisa de satisfação, conferência pública do documento assinado (o QR leva a uma página da Crommos, que mostra quem assinou e, com assinatura ICP-Brasil, entrega o PDF), importação de dados (o arquivo não é guardado) e a agenda no celular (o calendário do médico — Google, Apple, Microsoft — busca a agenda pelo link dele; por padrão o título é

só "Consulta"; o provedor do calendário é escolha do profissional, não suboperador). A contagem da franquia de teleconsultas vai do Crommos Clinic à plataforma de cobrança da Crommos só com o código do atendimento.

A **transcrição local da consulta**, recurso do Prontuário, roda no navegador do médico: o áudio não vai a terceiro nenhum. Os arquivos dos modelos (Whisper, para transcrever, e Qwen3, para organizar o texto nos campos) são baixados uma vez de um repositório público, o **Hugging Face** (EUA), que só entrega arquivos estáticos e não recebe dado de paciente — vê apenas o endereço IP do computador no download. Por isso não é suboperador. Para eliminar até isso, a Crommos pode passar a servir esses arquivos pelo próprio aplicativo.

Consultas que o navegador faz direto a serviços públicos, sem contrato e sem dado de saúde:

- **ViaCEP** (Brasil): ao digitar o CEP no cadastro do paciente, da clínica ou da unidade, o navegador envia **só o CEP** para completar o endereço. O serviço vê o CEP e o IP de quem digita, sem nome nem outro dado do paciente.

As letras da tela (fonte Montserrat) são servidas pelo próprio aplicativo: o navegador da equipe e do paciente não busca fonte em serviço externo.

Obrigações da Crommos sobre esta lista

- Manter a lista atualizada e **avisar a clínica com 30 dias de antecedência** antes de incluir ou trocar suboperador, com direito de objeção (DPA, cláusula 7).
- Contrato com cada suboperador com obrigações de proteção equivalentes às do DPA (art. 39).
- Transferência internacional (itens 3, 4 e 5) com as cláusulas-padrão contratuais da ANPD, na íntegra e sem alteração (art. 33, II, "b"; Res. CD/ANPD 19/2024, art. 16), assinadas antes do primeiro envio de dado, e cópia delas à clínica que pedir, para ela atender o titular (art. 17). O fornecedor que não aceitar as cláusulas é trocado, com o aviso da cláusula 7 do DPA.
- Nenhum dado clínico sai para os itens 4, 5 e 9. Aos itens 7 e 8 vai só o código (hash) do documento.

Fontes

- Daily — Data Processing Addendum e Proteção de dados.
- Resend — Choosing a Region, Data Processing Addendum e Pricing (retenção de dados).
- Meta — WhatsApp Cloud API: local storage e Data privacy & security.
- Memed — Política de Segurança e Política de Privacidade — Médicos.
- AbacatePay — Termos e Política de Privacidade.
- Asaas — Termos e Condições de Uso e Política de Privacidade (links do rodapé de asaas.com, conferidos em 31/10/2026).
- Efí — Termos e contratos e Política de Privacidade.
- Stripe — Contrato de serviços (Brasil) e Política de Privacidade.