

Contrato de Operação de Dados (DPA)

Plataforma ClinIQ - Gestão para Clínicas

Objetivo: Este documento formaliza que a plataforma ClinIQ trata os dados sensíveis de saúde (prontuários e informações de pacientes) exclusivamente na qualidade de **Operador**, atuando estritamente sob as instruções do profissional de saúde ou clínica (o **Controlador**).

Este Contrato de Operação de Dados ("DPA") regula o tratamento de dados pessoais de pacientes realizado pelo sistema **ClinIQ** ("OPERADOR") em nome do profissional cadastrado na Plataforma ("CONTROLADOR"), de acordo com os termos do art. 39 da Lei 13.709/2018 (Lei Geral de Proteção de Dados - LGPD).

1. Definições

- **CONTROLADOR:** O profissional de saúde ou clínica que utiliza o sistema e que define a finalidade e os meios do tratamento dos dados de seus pacientes.
- **OPERADOR:** O sistema ClinIQ, responsável por processar e armazenar os dados dos pacientes exclusivamente conforme as diretrizes do Controlador.
- **TITULAR:** A pessoa natural (paciente) a quem se referem os dados pessoais que são tratados no sistema.
- **DADOS PESSOAIS:** Qualquer informação relacionada ao paciente, incluindo os dados sensíveis de saúde definidos no art. 5º, II da LGPD.

2. Objeto do Tratamento

O Operador compromete-se a tratar os Dados Pessoais dos pacientes inseridos pelo Controlador exclusivamente para garantir o pleno funcionamento dos módulos da plataforma ClinIQ (como armazenamento de prontuários eletrônicos, agendamento de consultas, gestão financeira e emissão de laudos), conforme as ações realizadas pelo Controlador no uso padrão do sistema.

3. Obrigações e Deveres do Operador (Cliniq)

- Realizar o tratamento de Dados Pessoais estritamente para a execução das funcionalidades do sistema, abstendo-se de utilizá-los para finalidades externas, campanhas de marketing ou treinamento de inteligência artificial, salvo mediante prévia e expressa autorização.
- Assegurar que toda a infraestrutura técnica mantenha os dados sob rígido sigilo e obrigações de confidencialidade.
- Implementar medidas de segurança da informação apropriadas para blindar os dados contra acessos não autorizados, vazamentos, destruição acidental ou ilícita e qualquer forma de tratamento inadequado.
- Comunicar o Controlador de forma célere e transparente acerca de qualquer incidente de segurança que possa representar risco ou dano aos pacientes.
- Prover as ferramentas necessárias para auxiliar o Controlador no atendimento aos direitos dos titulares (como exportação, correção e exclusão de prontuários).
- Garantir a exclusão ou devolução estruturada de todos os dados ao fim do período de utilização da plataforma, ressalvada a necessidade de retenção por exigência técnica de transição ou determinação legal.

4. Obrigações e Deveres do Controlador (Profissional/Clínica)

- Assegurar que possui amparo legal válido e legítimo para a coleta e o registro dos dados de seus pacientes na plataforma (como o consentimento do paciente ou a tutela da saúde).
- Manter a exatidão e a qualidade das informações clínicas inseridas no prontuário.
- Prestar os devidos esclarecimentos aos seus pacientes acerca de como seus dados são geridos no consultório e armazenados sistemicamente.

5. Subcontratação e Infraestrutura

Para garantir a alta disponibilidade e a segurança do serviço, o Operador conta com provedores de infraestrutura de classe mundial (como serviços de hospedagem e processamento de pagamentos). O Operador assume a responsabilidade de garantir que estes provedores operem com os mesmos padrões de segurança e sigilo exigidos pela LGPD, ressaltando que processadores de pagamento não possuem qualquer tipo de acesso aos dados clínicos ou prontuários dos pacientes.

6. Medidas de Segurança da Informação

O sistema adota um conjunto rigoroso de controles técnicos, incluindo:

- Isolamento lógico de banco de dados, garantindo que as informações de um Controlador jamais se misturem com as de outro.
- Criptografia de dados em trânsito ponta a ponta (Protocolos HTTPS/TLS).
- Armazenamento de credenciais de acesso por meio de funções de *hash* irreversíveis.
- Controle rigoroso de autenticação e rotinas de backup para prevenção contra perda de dados.

7. Vigência e Disposições Finais

O presente DPA entra em vigor no momento do cadastro do Controlador na plataforma e permanecerá válido durante todo o período de utilização do sistema. Após o encerramento da conta, o Operador garantirá um prazo para a exportação completa dos dados pelo Controlador antes de proceder com o apagamento definitivo e irreversível dos registros nos servidores.