

Política de Coleta e Processamento de Dados Pessoais

Clínica Médica: UMCP LDA

NIF 519073800

Data de Entrada em Vigor: 27 de abril de 2026

Última Atualização: 27 de abril de 2026

Seção 1: Informações Gerais

- Nome Completo: UMCP LDA
NIF 519073800
- Endereço: R. do Dr. Alfredo Magalhães 90, 4000-290 Porto
- Informações de Contato: admin@umedclinic.pt, 913836059
- Responsável pela Proteção de Dados: Não designado ainda (informações serão atualizadas após a designação).

A clínica compromete-se a cumprir o Regulamento Geral de Proteção de Dados (RGPD) e a legislação portuguesa sobre proteção de dados pessoais.

Seção 2: Finalidades do Processamento de Dados

A clínica processa dados pessoais exclusivamente para as seguintes finalidades:

- Prestação de Serviços Médicos:
 - Diagnóstico, tratamento e prevenção de doenças.
 - Manutenção de registros médicos e históricos de saúde.
 - Prescrição de medicamentos, vacinação e monitoramento da saúde.
- Gestão Administrativa:
 - Registro de pacientes e agendamento de consultas.
 - Manutenção de registros, faturamento e interação com seguradoras.
 - Lembretes de consultas e notificações de resultados de exames.
- Obrigações Legais e Regulatórias:
 - Relatórios às autoridades reguladoras de saúde.
 - Cumprimento de exigências de programas nacionais de saúde.
- Proteção de Interesses Vitais:
 - Resposta a emergências.
 - Contato com parentes em situações de risco à vida.
- Segurança de Dados e Ordem Interna:
 - Controle de acesso a registros médicos.
 - Uso de videomonitoramento (se aplicável).
- Pesquisas Científicas e Educação (Dados Anonimizados):
 - Uso de dados anonimizados para treinamento e análise.
- Serviços de Telemedicina (se aplicável):
 - Realização de consultas remotas.
- Marketing (com consentimento do paciente):
 - Notificações sobre novos serviços da clínica.

Seção 3: Categorias de Dados Processados

- Dados Gerais:
 - Nome completo, data de nascimento, gênero.
 - Endereço, informações de contato (telefone, e-mail).
 - Documentos de identificação (passaporte, ID).
- Dados Sensíveis:

- Histórico de saúde, diagnósticos, resultados de exames, tratamentos prescritos.
- Doenças crônicas, gravidez, detalhes de vacinação.
- Alergias, receitas médicas, intervenções cirúrgicas.
- Dados Administrativos:
 - Número de identificação do paciente no sistema.
 - Dados de seguro (número da apólice, seguradora).
- Informações de Pagamento:
 - Histórico de pagamentos, documentos financeiros.
- Dados Adicionais com Consentimento do Paciente:
 - Fotos, vídeos para documentação médica.
 - Participação em pesquisas científicas.

Seção 4: Fontes de Dados

- Pacientes: Dados fornecidos no registro, verbalmente ou via plataformas digitais.
- Instituições Médicas: Encaminhamentos de médicos, laboratórios ou outras clínicas.
- Seguradoras: Informações sobre apólices e coberturas.
- Autoridades Governamentais: Dados de registros e relatórios obrigatórios.
- Família do Paciente: Contatos de emergência.
- Sistemas Automatizados: Sistemas de telemedicina e monitoramento.

Seção 5: Armazenamento de Dados

- Locais de Armazenamento:
 - Dados eletrônicos: Servidores criptografados na UE e armazenamento em nuvem compatível com RGPD.
 - Arquivos em papel: Instalados em locais trancados com acesso restrito.
- Períodos de Retenção:
 - Registros médicos: Pelo menos 10 anos após o término do tratamento, conforme legislação portuguesa.
 - Registros financeiros: 5 anos (para conformidade fiscal).
 - Dados de videomonitoramento: Até 30 dias, se utilizado.
- Medidas de Proteção:
 - Criptografia de dados, controle de acesso e ferramentas de cibersegurança.

Seção 6: Base Legal para o Processamento de Dados

- Consentimento do Paciente:
 - Para processar categorias especiais de dados (sensíveis).
 - Para uso de dados em marketing ou pesquisas.
- Cumprimento de Contrato: Prestação de serviços médicos.
- Obrigações Legais: Cumprimento das leis nacionais.

Seção 7: Sistemas de Informação Utilizados

A clínica utiliza o sistema de informação médica certificado iMed para gerenciar, armazenar e processar os dados dos pacientes.

Características do Sistema iMed:

- Finalidades de Uso:
 - Manutenção de registros médicos eletrônicos.
 - Gestão de agendamentos de pacientes.
 - Processamento de dados de diagnóstico, resultados laboratoriais e prescrições.
 - Armazenamento de históricos de saúde.

- Organização de serviços de telemedicina (se aplicável).
- Análise de dados para melhoria interna dos serviços médicos.
- Segurança dos Dados:
 - Criptografia: Dados criptografados em armazenamento e transmissão.
 - Controle de Acesso: Apenas pessoal autorizado tem acesso baseado em funções.
 - Registro de Ações: Manutenção de logs completos para rastreamento de dados.
 - Backup: Dados são regularmente armazenados em servidores compatíveis com RGPD dentro do EEE.
- Direitos dos Pacientes:
 - iMed suporta solicitações de acesso, correção, exclusão (quando justificável) e restrição de processamento.
 - Pacientes podem solicitar documentação médica em formato estruturado.
 - Retenção de Dados:
 - Dados médicos armazenados em servidores seguros na UE, em conformidade com o RGPD.
 - Documentos em papel armazenados em instalações protegidas da clínica.
- Obrigações Contratuais:
 - A clínica possui um contrato com o provedor do iMed, garantindo conformidade com o RGPD e definindo responsabilidades para notificação de violações de dados e medidas protetivas.

Seção 8: Resposta a Incidentes

Em caso de violação de dados envolvendo o iMed:

- Notificação imediata ao provedor do iMed.
- Notificação ao CNPD em até 72 horas.
- Informação aos indivíduos afetados, caso exista alto risco aos seus direitos e liberdades.

Seção 9: Direitos dos Pacientes

Os pacientes têm o direito de:

- Acessar seus dados.
- Solicitar correções de imprecisões.
- Solicitar exclusão de dados (quando legalmente permitido).
- Restringir o processamento de dados.
- Registrar reclamações no CNPD.

Para exercer esses direitos, os pacientes podem contatar: admin@umedclinic.pt

Seção 10: Compartilhamento de Dados com Terceiros

- Destinatários:
 - Seguradoras (processamento de apólices).
 - Autoridades governamentais (para relatórios).
 - Laboratórios e centros de diagnóstico.
- Medidas de Proteção:
 - Contratos de processamento de dados.
 - Verificação de conformidade com o RGPD.

Seção 11: Resposta a Incidentes

- Notificar CNPD e indivíduos afetados em até 72 horas.
- Realizar investigação interna.
- Implementar medidas corretivas para prevenir recorrências.