ENMED
Saúde e Segurança do Trabalho

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Diretrizes básicas de proteção e uso responsável da informação
em conformidade com a LGPD e os requisitos da API Oficial da Meta

CNPJ: 27.510.562/0001-31
Razão Social: Enmed Saúde e Segurança do Trabalho LTDA
Site: enmed.com.br
Montes Claros – MG

Versão 1.0 | 30 de abril de 2025

1. Objetivo e Escopo

Esta Política de Segurança da Informação estabelece as diretrizes básicas adotadas pela Enmed Saúde e Segurança do Trabalho LTDA para proteger as informações de seus clientes, colaboradores e parceiros, bem como para assegurar a confidencialidade, integridade e disponibilidade dos dados tratados pela empresa.

Esta Política aplica-se a todos os colaboradores, prestadores de serviço e parceiros que tenham acesso a informações da Enmed ou de seus clientes, e atende aos requisitos de segurança da API Oficial do WhatsApp Business da Meta Platforms, Inc. e às disposições da Lei Geral de Proteção de Dados (LGPD).

2. Princípios de Segurança

A Enmed baseia sua abordagem de segurança nos seguintes princípios fundamentais:

Princípio	Descrição
Confidencialidade	As informações são acessadas somente por pessoas autorizadas e com necessidade justificada.
Integridade	As informações são mantidas precisas, completas e protegidas contra alterações não autorizadas.
Disponibilidade	As informações e sistemas são acessíveis às pessoas autorizadas quando necessário.
Responsabilidade	Todo acesso a dados é atribuído a um responsável identificado.
Minimização	Somente os dados estritamente necessários para cada finalidade são coletados e tratados.

3. Controle de Acesso

O acesso a dados pessoais de clientes e a informações confidenciais da Enmed é controlado da seguinte forma:

- O acesso é concedido somente a colaboradores e prestadores que necessitem das informações para o desempenho de suas funções específicas (princípio do menor privilégio).
- Cada colaborador possui credenciais de acesso individuais e intransferíveis para as plataformas utilizadas na operação da Enmed.
- O compartilhamento de credenciais entre colaboradores é expressamente vedado.
- Acessos são revisados periodicamente; ao término de vínculo com a Enmed, as credenciais são revogadas imediatamente.
- Dispositivos utilizados para acesso a dados de clientes devem estar protegidos por mecanismos de autenticação adequados, incluindo o uso de autenticação em dois fatores (2FA) sempre que disponível nas plataformas utilizadas.
- A Enmed incentiva o uso de credenciais de acesso cuidadosamente criadas, com combinação de letras, números e caracteres especiais, e orienta todos os usuários a evitarem o reaproveitamento de senhas entre plataformas distintas.

4. Proteção de Dados no WhatsApp Business (Meta)

Em razão do uso da API Oficial do WhatsApp Business, a Enmed adota as seguintes medidas específicas:

- Apenas colaboradores autorizados têm acesso à plataforma de atendimento integrada ao WhatsApp Business API.
- As conversas com clientes são tratadas com sigilo profissional; seu conteúdo não é divulgado a terceiros sem base legal ou consentimento do titular.
- O número oficial do WhatsApp Business da Enmed é utilizado exclusivamente para fins de atendimento, agendamento, suporte e comunicações relacionadas aos serviços prestados.
- O acesso ao painel de gerenciamento da API Meta é protegido por autenticação segura e restrito às pessoas com atribuição direta nessa função.
- Não é permitido o uso do número ou da conta oficial para comunicações pessoais, publicidade não autorizada ou qualquer finalidade fora do escopo dos serviços da Enmed.

5. Uso de Plataformas e Sistemas de Terceiros

A Enmed não possui sistema próprio de gestão; toda a operação é realizada por meio de plataformas e sistemas de terceiros especializados, contratados para suporte às suas atividades. Nesse contexto:

- A responsabilidade pela segurança, manutenção, disponibilidade e controles internos dos sistemas utilizados (incluindo controles de auditoria e registros de operações) é dos respectivos fornecedores e prestadores de serviço de tecnologia.
- A Enmed exige, em seus contratos com prestadores de tecnologia, cláusulas de confidencialidade, proteção de dados e conformidade com a LGPD.
- Incidentes de segurança em plataformas de terceiros devem ser imediatamente reportados ao prestador responsável pelo sistema afetado.
- Qualquer integração de novos sistemas ou plataformas que envolvam tratamento de dados pessoais de clientes deverá ser avaliada previamente quanto aos aspectos de segurança e conformidade.

6. Transmissão e Armazenamento Seguro de Dados

- Dados pessoais de clientes não devem ser transmitidos por canais não criptografados ou sem as devidas proteções.
- O envio de informações sensíveis (laudos, dados financeiros, documentos pessoais) entre a Enmed e clientes é realizado por canais seguros, preferencialmente os disponibilizados pelas plataformas contratadas.
- Documentos físicos e digitais contendo dados pessoais são armazenados em locais e ambientes de acesso restrito.
- Backups e cópias de segurança de dados críticos, quando aplicáveis, são de responsabilidade dos prestadores de sistema contratados.

7. Uso de Dispositivos e Ambientes de Trabalho

- Dispositivos utilizados para acesso a dados de clientes (computadores, tablets, smartphones) devem ter tela bloqueada automaticamente quando não utilizados.
- O acesso a dados de clientes em redes públicas ou abertas de Wi-Fi deve ser evitado; quando necessário, recomenda-se o uso de conexões VPN ou plano de dados móvel.
- Softwares de proteção (antivírus, atualizações de sistema operacional) devem ser mantidos atualizados nos dispositivos utilizados para operação da Enmed.

- A instalação de aplicativos não autorizados ou suspeitos em dispositivos utilizados para operação é vedada.

8. Incidentes de Segurança

Qualquer suspeita ou confirmação de incidente de segurança envolvendo dados da Enmed ou de seus clientes deve ser tratada com prioridade:

1. Identificação e contenção imediata do incidente;
2. Comunicação imediata à gestão da Enmed;
3. Acionamento do prestador de serviço de tecnologia responsável pelo sistema afetado;
4. Avaliação do impacto sobre dados pessoais de titulares;
5. Notificação à ANPD e aos titulares afetados, quando exigido pela LGPD (prazo de até 72 horas para notificação à autoridade em casos de alto risco);
6. Registro do incidente e das ações adotadas para prevenção de recorrência.

9. Engenharia Social e Phishing

A Enmed orienta seus colaboradores a:

- Não fornecer credenciais de acesso, senhas ou dados de clientes mediante solicitação por e-mail, mensagem ou telefone não verificado;
- Verificar a autenticidade de comunicações suspeitas antes de clicar em links ou abrir arquivos;
- Reportar imediatamente à gestão qualquer tentativa suspeita de obtenção de informações por terceiros.

10. Dados Sensíveis de Saúde Ocupacional

A Enmed, por sua natureza de atuação em medicina e segurança do trabalho, pode ter acesso a dados sensíveis de saúde no contexto de exames ocupacionais realizados para empresas-clientes. Para esses dados, aplicam-se medidas adicionais:

- O acesso é restrito aos profissionais de saúde diretamente envolvidos no atendimento;
- Resultados de exames e laudos são compartilhados estritamente nos limites da legislação trabalhista e de saúde ocupacional vigente;
- O tratamento de dados de saúde segue o Art. 11 da LGPD, que exige base legal específica.

11. Responsabilidades

Parte	Responsabilidade
Gestão da Enmed	Aprovar, comunicar e garantir o cumprimento desta Política; avaliar incidentes; manter contratos de confidencialidade com fornecedores.
Colaboradores e prestadores internos	Seguir as diretrizes desta Política; proteger credenciais de acesso; reportar incidentes.
Prestadores de sistemas e tecnologia	Manter a segurança, disponibilidade e integridade das plataformas fornecidas; cumprir as cláusulas contratuais de proteção de dados.

12. Vigência e Revisão

Esta Política entra em vigor na data de sua publicação e será revisada pelo menos anualmente, ou sempre que ocorram mudanças relevantes nas operações, tecnologias utilizadas ou na legislação aplicável. A versão vigente será sempre disponibilizada em enmed.com.br.

13. Contato

Dúvidas sobre esta Política ou relatos de incidentes de segurança:
E-mail: privacidade@enmed.com.br
Site: enmed.com.br
Endereço: Rua João F. Pimenta, 215, Cidade Santa Maria, Montes Claros – MG, CEP 39.401-081
Versão 1.0	30 de abril de 2025