	<b>DOCUMENTO</b> ANEXO Á POLÍTICA DE IA	Código: DOC_TI_400
		Data de Emissão: 07/11/2025
	<b>GUIA DE BOAS PRÁTICAS: USO DE INTELIGÊNCIA ARTIFICIAL (IA)</b>	Data da Revisão: 07/11/2026
		Revisão Nº: 01

Manter a privacidade e a segurança dos dados também é parte da sua rotina, e isso se torna ainda mais crítico com o uso crescente de ferramentas de Inteligência Artificial. Este guia traz orientações simples, mas essenciais, para proteger informações sensíveis ao interagir com sistemas de IA.

### Por que isso é importante?


- ✓ Reduz o risco de vazamento de informações sigilosas ou propriedade intelectual, impedindo que os dados sejam usados no treinamento do modelo de IA.
- ✓ Evita o acesso indevido por terceiros (a empresa provedora da IA e seus funcionários) a detalhes estratégicos ou pessoais inseridos.
- ✓ Demonstra responsabilidade e cuidado com os dados dos nossos pacientes, cooperados, parceiros e colegas ao garantir que não serão expostos em prompts públicos.
- ✓ Contribui para a conformidade com a LGPD (Lei Geral de Proteção de Dados), prevenindo o tratamento inadequado de dados pessoais por meio de ferramentas não autorizadas.

### Boas Práticas de Segurança e Privacidade no Uso de IA

Integrar a Inteligência Artificial ao seu trabalho exige uma atenção redobrada com as informações que você manipula. Seguindo práticas essenciais para proteger dados sensíveis, tanto no ambiente físico quanto nas interações com ferramentas de IA, o maior risco com IA está no que você compartilha. Garanta que seus prompts e inputs estejam livres de dados sensíveis:

#### 1. Nunca insira informações confidenciais:

- ✓ **Restrição Absoluta:** Jamais cole ou digite dados pessoais identificáveis (CPF, nome completo de clientes/pacientes), propriedade intelectual da empresa, códigos-fonte sigilosos, ou quaisquer informações estratégicas em ferramentas de IA generativa públicas.
- ✓ **Dados para Treinamento:** Lembre-se que muitas IAs utilizam o seu input para treinar seus modelos, tornando o risco de vazamento ou exposição permanente.

	<b>DOCUMENTO</b> ANEXO À POLÍTICA DE IA	Código: DOC_TI_400
		Data de Emissão: 07/11/2025
	<b>GUIA DE BOAS PRÁTICAS: USO DE INTELIGÊNCIA ARTIFICIAL (IA)</b>	Data da Revisão: 07/11/2026
		Revisão Nº: 01

## 2. Use a Anonimização:


- ✓ Se for imprescindível usar a IA para processar um texto baseado em dados reais, **remova ou substitua** todas as informações sensíveis (nomes, datas, valores exatos) por dados genéricos ou fictícios.

## 3. Acultramento em Segurança e Privacidade:

- ✓ **Jornada Contínua:** Em 12 meses, promover no mínimo 2 treinamentos, palestras e comunicados para reforçar a cultura de segurança. E garantir que toda a equipe esteja atualizada sobre as melhores práticas de proteção de dados com vídeos curtos. Para gerar menos riscos de vazamento, maior proteção aos dados de nossos clientes/pacientes e conformidade total com a LGPD.

### Dicas Extras

- ✓ Pense antes de digitar: Qualquer informação inserida na IA, pode ser considerada pública ou usada para treinamento. Se for sensível, não digite.
  - ✓ Use a IA como rascunho, não como final: O conteúdo gerado deve ser o ponto de partida, não o ponto final. A responsabilidade da verificação é sempre sua.
  - ✓ Se a IA te pedir, desconfie: Sistemas de IA legítimos não solicitam senhas ou informações altamente sigilosas (como chaves de API, segredos de negócio ou dados bancários completos).
  - ✓ Mantenha sua curiosidade profissional, mas segura: Explore as ferramentas de IA, mas utilize apenas dados genéricos, públicos ou anonimizados em seus experimentos.
- **Lembre-se:** cada colaborador é peça-chave na proteção da informação! Seu cuidado com o prompt é a primeira linha de defesa contra vazamentos na era da Inteligência Artificial.

	<b>DOCUMENTO</b> ANEXO Á POLÍTICA DE IA	Código: DOC_TI_400
		Data de Emissão: 07/11/2025
	<b>GUIA DE BOAS PRÁTICAS: USO DE INTELIGÊNCIA ARTIFICIAL (IA)</b>	Data da Revisão: 07/11/2026
		Revisão Nº: 01

**Em caso de dúvidas ou para relatar qualquer situação de risco:**

Entre em contato com o Encarregado de Dados (DPO) ou o Comitê de Segurança da Informação da sua unidade.

- Este material é parte das ações do Programa de Governança em Proteção de Dados e Segurança da Informação da Unimed.

***Mantenha este guia visível e pratique diariamente.***

Drº Antônio Carlos Andrade  
Presidente  
Unimed de Tupã