Boas Práticas de Governança em Privacidade

PARA COLABORADORES E TERCEIROS DO INSTITUTO SOCIAL MAIS SAÚDE

Privacidade e proteção de dados: um compromisso com a ética e o respeito

INSTITUTO
Mais
Saúde

Apresentação

No Instituto Social Mais Saúde (ISMS), proteger a privacidade dos dados pessoais de pacientes, colaboradores e terceiros é um dever de todos. Esta cartilha tem como objetivo orientar você sobre as boas práticas no tratamento de dados pessoais no ambiente hospitalar, garantindo conformidade com a Lei Geral de Proteção de Dados (LGPD) e a nossa Política de Governança de Dados Pessoais.

1. O que são dados pessoais?

Dados pessoais são quaisquer informações que identificam ou possam identificar uma pessoa, como:

» Nome, RG, CPF;
» Endereço, telefone, e-mail;
» Dados de saúde e prontuários médicos.

Dados pessoais sensíveis, que exigem maior proteção, incluem:

» Origem racial ou étnica;
» Informações sobre saúde ou genética;
» Convicções religiosas ou filosóficas.

2. Princípios para o tratamento de dados pessoais

Ao tratar dados pessoais, siga sempre os princípios da LGPD:

- **Finalidade**: Use dados apenas para objetivos claros e legítimos.
- **Necessidade**: Colete somente os dados indispensáveis.
- **Transparência**: Informe ao titular como seus dados serão usados.
- **Segurança**: Proteja os dados contra acessos não autorizados.

3. Exemplos práticos de boas práticas no tratamento de dados pessoais

Cenário 1: **Atendimento ao Paciente**

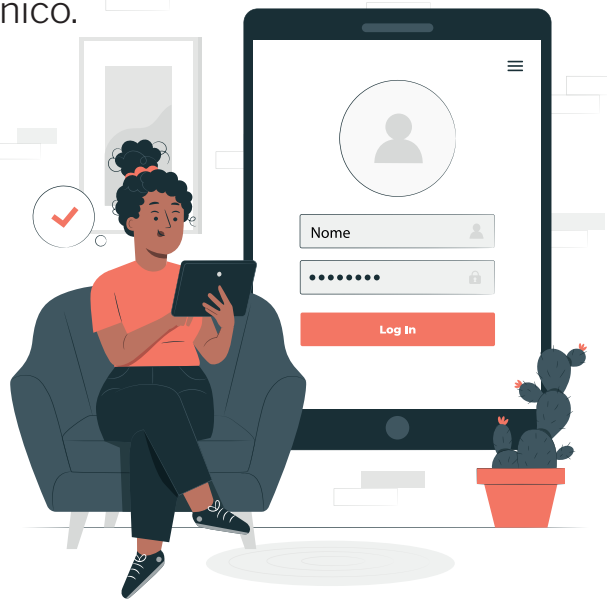
Errado: Divulgar informações médicas de um paciente em locais públicos ou acessíveis a outros pacientes.

Certo: Garantir que informações de saúde sejam compartilhadas apenas com profissionais autorizados e em locais seguros, como em salas fechadas ou através de sistemas protegidos.

Cenário 2: **Uso de Sistemas Eletrônicos**

Errado: Compartilhar login e senha para acesso ao prontuário eletrônico.

Certo: Manter sua senha em sigilo e não acessar prontuários sem autorização ou necessidade.



Cenário 3: **Documentação Física**

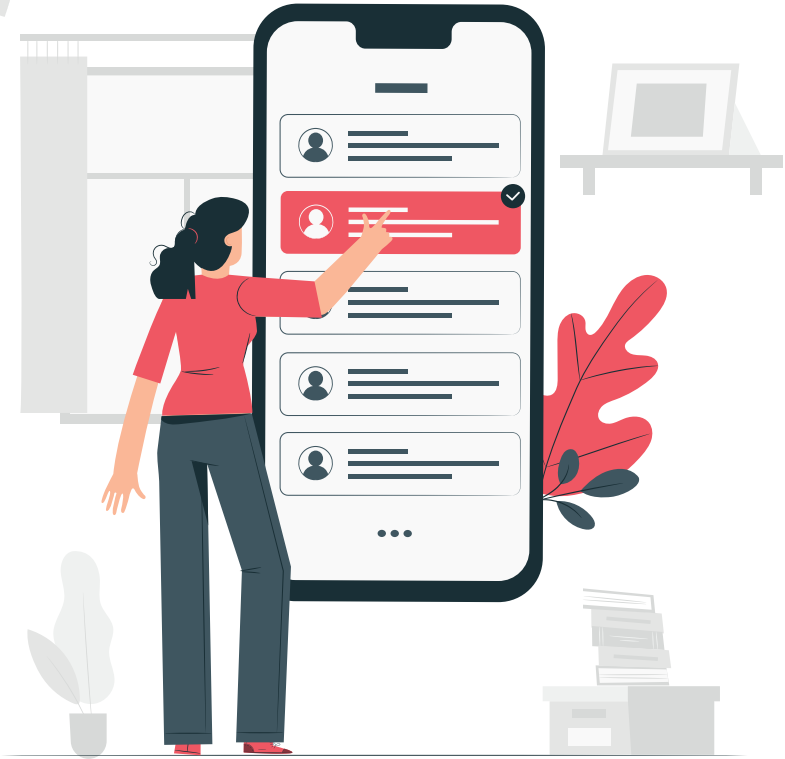
Errado: Deixar fichas de cadastro de pacientes ou documentos médicos em locais desprotegidos.

Certo: Armazenar documentos físicos em armários trancados e destruir cópias que não sejam mais necessárias de maneira segura.

Cenário 4: **Comunicação de Dados**

Errado: Enviar informações de saúde por aplicativos de mensagens sem proteção.

Certo: Usar plataformas seguras e autorizadas para a comunicação interna de informações sensíveis.



4. Boas práticas para colaboradores e terceiros

Para todos os profissionais:

» Evite o uso de dispositivos pessoais: Não armazene informações de pacientes ou documentos do hospital em seus dispositivos pessoais.

» Respeite as áreas de acesso: Não acesse locais físicos ou sistemas que não sejam de sua competência.

» Cuidado com e-mails e links suspeitos: Evite phishing e outros ataques que podem comprometer a segurança dos dados.

Para quem trata dados de saúde (médicos, enfermeiros, farmacêuticos...):

» Solicite o consentimento do paciente para tratamentos não previstos pela legislação.

» Documente de forma clara e acessível as ações realizadas.

» Revise regularmente os dados de pacientes para garantir sua exatidão.

Para quem trabalha na recepção ou atendimento:

» Solicite apenas as informações necessárias ao atendimento.

» Oriente os pacientes sobre como suas informações serão utilizadas.

» Não comente detalhes sobre pacientes com outros colegas, exceto os diretamente envolvidos no atendimento.

5. Consequências do tratamento inadequado de dados

O uso indevido ou vazamento de dados pessoais pode gerar:

» ***Sanções legais***: Multas e penalidades impostas pela ANPD.

» ***Perda de confiança***: Comprometimento da reputação do Instituto Social Mais Saúde e de seus profissionais.

» ***Impactos financeiros e operacionais***: Custos com correções, indenizações e medidas corretivas.

6. Direitos dos titulares de dados pessoais

Todo indivíduo tem o direito de:

Acessar os dados que o Instituto Social Mais Saúde mantém sobre ele;

» Solicitar correções em informações incorretas;

» Revogar consentimentos previamente fornecidos;

» Solicitar a exclusão de dados, quando aplicável.

Os titulares podem registrar pedidos no site do Instituto Social Mais Saúde (www.institutomaissaude.org.br) ou enviar um e-mail para **dpo@ismsaude.org.br**.

7. Como reportar incidentes?

Caso identifique um possível incidente de segurança (exemplo: acesso indevido, vazamento de dados), informe imediatamente:

» Encarregado de Dados Pessoais (DPO): **dpo@ismsaude.org.br**

» Área de TI: [e-mail ou canal interno].

O quanto antes agirmos, menores serão os riscos para o Instituto Social Mais Saúde e para os titulares dos dados.

8. Juntos pela privacidade e segurança

A proteção de dados pessoais no ambiente hospitalar exige a colaboração de todos. Ao seguir essas boas práticas, você contribui para um ambiente mais seguro e ético, reforçando a confiança que nossos pacientes, colaboradores e parceiros depositam no Instituto Social Mais Saude.

BOAS PRÁTICAS DE GOVERNANÇA EM PRIVACIDADE

Conheça nosso Portal de Privacidade
www.institutomaissaude.org.br/privacidade

Ou envie suas dúvidas para:
dpo@ismsaude.org.br

Privacidade e proteção de dados: um compromisso com a ética e o respeito

@institutosocialmaissaude

www.institutomaissaude.org.br

INSTITUTO Mais Saúde