

CARTILHA

SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS DO PACIENTE



Por que esta cartilha existe?

i

Todos os dias, lidamos com informações importantes sobre nossos **clientes, colaboradores e parceiros**.



Proteger esses dados é uma responsabilidade de **TODOS**.



Quando preservamos a confidencialidade, a integridade e a disponibilidade das informações, fortalecemos a **confiança** dos nossos clientes e garantimos uma assistência **segura e ética**.



O que é Política de Segurança?

A Política de **Segurança para a Tecnologia da informação** aplica-se a **todos os funcionários, prestadores de serviços, sistemas e serviços**, incluindo trabalhos executados externamente ou por terceiros, que **utilizem o ambiente de processamento do Amaral Costa Medicina Diagnóstica** ou **acesso às informações** pertencentes ao mesmo.

Todo e qualquer usuário de recursos computadorizados do Amaral Costa Medicina Diagnóstica tem a **responsabilidade pela segurança e integridade das informações** e pelos **equipamentos de informática**.



A violação desta política de segurança é qualquer ato que:

1

Exponha o Laboratório a uma **perda monetária** efetiva ou potencial por meio do comprometimento da segurança dos dados e/ou de informações ou ainda pela perda de equipamento.

2

Envolve a **revelação de dados confidenciais**, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.

3

Envolve o uso de dados para **propósitos ilícitos** que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.



O que são Dados pessoais?

São informações que podem **identificar uma pessoa**, diretamente ou em combinação com outras informações.



DADOS PESSOAIS

Informações que **identificam** você.



Nome



CPF



Telefone



Endereço



E-mail



Imagem



Voz



Número do convênio



Ordem de Serviço



E DADOS SENSÍVEIS?

Informações mais delicadas, que exigem ainda **mais cuidado**.



Resultado de exames



Formulário de exames



Patologias



Gestação



Dados genéticos



Biometria

Cada colaborador faz a diferença

Pequenas atitudes no dia a dia **protegem as informações** dos nossos clientes, colaboradores e parceiros, e **fortalecem a confiança** em nosso trabalho.



✓ RECOMENDAMOS



Use apenas seu login.

Seu acesso é pessoal e intransferível.



Mantenha sua senha em segredo.

Não compartilhe com ninguém.



Bloqueie o computador ao se ausentar.

Proteja as informações mesmo na sua ausência.



Informe imediatamente qualquer incidente ao TI.

A comunicação rápida evita riscos maiores.



Guarde documentos corretamente.

Mantenha documentos impressos em local seguro e nunca os deixe expostos.



Utilize apenas sistemas autorizados.

Acesse somente ferramentas aprovadas pelo Amaral Costa.



Mantenha a mesa limpa.

Evite deixar documentos ou informações sobre a mesa.

O que nunca devemos fazer?

Alguns comportamentos podem comprometer a **confidencialidade das informações** e colocar em **risco a segurança dos dados dos pacientes**. Evite essas práticas.



X NÃO PERMITIDO



Compartilhar **senha**.



Fotografar exames.



Enviar resultados pelo **WhatsApp** pessoal.



Compartilhar **dados pessoais** de clientes.
(ex.: e-mail e telefone)



Consultar **resultados de pacientes**, sem necessidade.



Usar **pendrives** particulares.



Compartilhar **login**.



Acessar **redes sociais** ou **sites** sem relação com o trabalho.



Comentar **casos** de **pacientes**.

Cuidado com golpes digitais

Como identificar:

- ✓  E-mails estranhos
- ✓  Links suspeitos
- ✓  Boletos para pagamento imediato
- ✓  Pedido de senha
- ✓  Arquivos desconhecidos

! Desconfie de mensagens inesperadas ou fora do padrão.

Não clique em links e não abra anexos de origem duvidosa.

Nunca informe suas senhas ou dados pessoais.

Na dúvida, **não clique, não responda** e comunique imediatamente o TI.

Nunca desative as proteções do TI.



Senhas seguras

Sua senha é a chave que protege suas informações e as dos nossos pacientes.

Crie senhas fortes e mantenha-as em segredo!



✓ UMA BOA SENHA:

- Aa** ✓ Letras maiúsculas
- aa** ✓ Minúsculas
- 189** ✓ Números
- !@#)** ✓ Caracteres especiais



Exemplo de senha forte:

Am@ralCOSTa!2024

Senha forte

Dica: use uma senha longa e única para cada sistema. Assim, você aumenta sua proteção!

👎 NÃO UTILIZE:

- ✗ Nome
- ✗ Nascimento
- ✗ Sequência
- ✗ Número de telefone
- ✗ amaralcosta

Guarde suas senhas apenas para você. Compartilhá-las é um **risco para todos**.

Protegendo os dados dos pacientes

Situações do dia a dia.

Segurança da informação não depende apenas da tecnologia.





Recepção

- ✓ Chamar o paciente com descrição.
- ✓ Não deixar fichas expostas.
- ✓ Evite anunciar em voz alta os exames sendo realizados.





Dica: fale baixo, chame pelo nome completo somente quando necessário.



Coleta

- ✓ Confirmar identidade.
- ✓ Manter documentos protegidos.



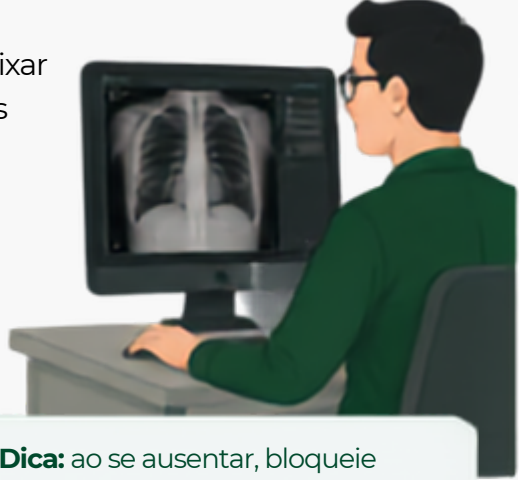


Dica: confire os dados com atenção e guarde os documentos de maneira adequada.



Imagem

- ✓ Não deixar exames visíveis.





Dica: ao se ausentar, bloqueie o sistema ou feche a tela.



Administrativo

- ✓ Compartilhar dados somente com quem tem direito de acesso.





Dica: valide a necessidade antes de enviar ou compartilhar qualquer informação.



TI

- ✓ Garantir acesso apenas para usuários autorizados.





Dica: revise acessos periodicamente e siga as políticas de segurança.

Se acontecer um incidente...

Incidentes podem acontecer.
O que importa é como reagimos.

Sua atitude rápida protege informações, pessoas e a reputação do **Amaral Costa**.



1



Percebi algo estranho

Identifique qualquer situação fora do normal, mesmo que pareça pequena.

2



Não tente resolver sozinho

Evite ações que possam piorar a situação ou comprometer as informações.

3



Comunique imediatamente

Informe o quanto antes para que possamos agir rápido e reduzir impactos.

4



TI + gestor

A informação será direcionada ao time de TI e ao seu gestor para análise.

5



Registro do incidente

O incidente será registrado para acompanhamento, tratamento e aprendizado.

6



Correção

Serão tomadas as ações necessárias para corrigir o problema e evitar novas ocorrências.

Comunicar é proteger.

Sua atitude faz a diferença na segurança da informação e na confiança dos nossos pacientes.

Seus direitos como titular dos dados

Respeitamos a sua privacidade e garantimos seus direitos de acordo com a legislação de proteção de dados.



Você pode:



Saber quais dados possuímos

Você pode saber quais dados pessoais tratamos.



Solicitar correção

Você pode pedir para corrigirmos dados completos, inexatos ou desatualizados.



Solicitar informações

Você pode solicitar informações sobre o tratamento dos seus dados.



Solicitar exclusão quando aplicável

Você pode pedir a exclusão dos seus dados, quando permitido por lei.



Solicitar portabilidade

Você pode solicitar uma cópia dos seus dados em formato estruturado.



Entrar em contato com o DPO

Você pode falar com nosso Encarregado de Proteção de Dados (DPO) sempre que precisar.



Seus dados são tratados com segurança, respeito e transparência.



Dúvidas ou solicitações?

Fale com o nosso DPO pelo e-mail: privacidade@amaralcosta.com.br

Segurança da Informação é uma construção conjunta entre o Departamento de TI e cada colaborador.

Contamos com você!

