CARTILHA:

PRINCÍPIOS

1. FINALIDADE
As informações coletadas precisam ter uma finalidade. Informe este objetivo ao titular de forma clara.

2. ADEQUAÇÃO
O tratamento das informações fornecidas precisa ser compatível com a finalidade informada ao titular.

3. NECESSIDADE
Apenas devem ser coletados dados que são necessários para a realização de suas finalidades.

4. LIVRE ACESSO
O titular deve ter livre acesso às suas informações pessoais e a maneira que estão sendo tratadas.

5. QUALIDADE DOS DADOS
Garantia, aos titulares, que os dados estão exatos e atualizados conforme a finalidade do tratamento.

6. TRANSPARÊNCIA
Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre o tratamento dos dados.

7. SEGURANÇA
Garante a segurança dos dados por meio de regras e recursos tecnológicos, para reduzir riscos de vazamento, perda de informações ou divulgação não permitida.

8. PREVENÇÃO
Adoção de medidas para prevenir a ocorrência de danos, como perda ou destruição de dados, entre outros.

9. NÃO DISCRIMINAÇÃO
Os dados nunca devem ser utilizados com fins discriminatórios, ilícitos e de má fé.

10. RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS
Demonstração de provas, pelo agente, da adoção de medidas eficazes para evitar qualquer descumprimento da Política de Segurança da Informação do Hospital Metropolitano Regional – PSI/HMR.

ATORES

HOSPITAL
Trata os dados dos pacientes.

GETÃO DE TI
Quem controla os dados.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS
ANPD
Órgão que fiscaliza a lei.

OFICIAL DE PROTEÇÃO DE DADOS
DPO
Pessoa que intermedia entre titular, ANPD e controlador.

PACIENTE
Pessoa que se refere os dados (dono).

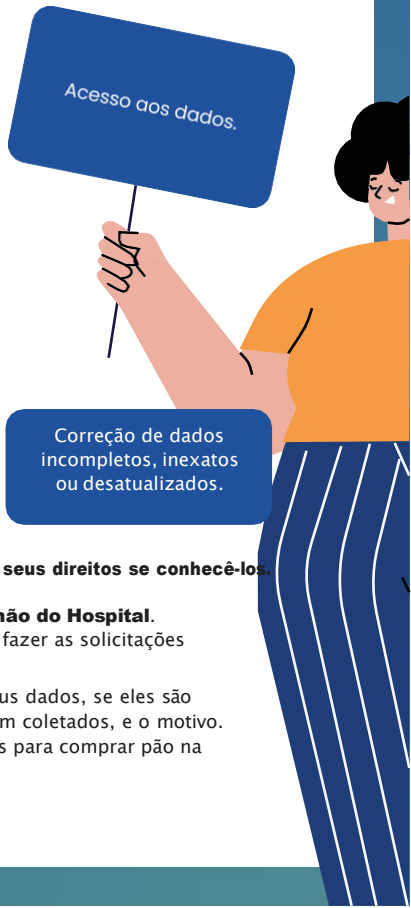
DADOS PESSOAIS

SENSÍVEIS	
Nome	Dados de Saúde
Telefone	Vida Sexual
Endereço	Opção Religiosa
RG/CPF	Opção Política
Salário	Cor/Raça
E-mail	Biometria

Os dados pessoais sensíveis podem causar discriminação a uma pessoa, por isso merecem maior proteção.

DIREITOS DOS PACIENTES

- Reclamação contra o Hospital junto à autoridade nacional.
- Eliminação de dados desnecessários, excessivos ou tratados em desconformidade.
- Oposição, caso discorde de um tratamento feito sem seu consentimento e o considere irregular.
- Confirmação da existência de tratamento dos dados.
- Ficar ciente da opção de negar consentimento para tratar os dados e compreender as possíveis consequências negativas da recusa.
- Portabilidade dos dados a outro fornecedor de serviço ou produto, observados os segredos comercial e industrial.
- Obter detalhes sobre as empresas com as quais o Hospital compartilhou os dados dos titulares.
- É possível excluir dados pessoais com consentimento, a menos que outra base legal permita seu uso contínuo, mesmo sem consentimento.
- Revogação do consentimento para tratar os dados pessoais.
- Correção de dados incompletos, inexatos ou desatualizados.



O paciente só poderá exercer seus direitos se conhecê-los.

Os dados são apenas seus, e **não do Hospital**.
Em toda empresa você poderá fazer as solicitações acima.

Questione quando pedirem seus dados, se eles são realmente necessários de serem coletados, e o motivo. Você irá passar seu CPF apenas para comprar pão na padaria? **Questione**.

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Acesso não autorizado no seu computador, e-mail, ou outros locais com login e senha individual.

Pessoa não autorizada acessou o celular ou notebook e teve acesso a dados de titulares e da empresa.

Extravio ou compartilhamento indevido de dados pessoais.

Envio de e-mail ao destinatário incorreto ou e-mail particular.

Deixar/encontrar papeis com dados pessoais na impressora ou mesa.

Funcionário copiando lista de contatos ou atendimentos para uso pessoal ou de terceiros.

Incidentes cibernéticos: invasão (hacker), vírus, comportamento anormal no computador (ransomware), e-mail de spam, e-mail solicitando dados como login/senha (phishing), etc.

Imagens divulgadas sem permissão (Ex: Redes sociais).

Perda de telefone, notebook, celular que utiliza para trabalho e possui dados de titulares ou confidenciais e sigilosos do hospital.

Bater foto do prontuário, cadastro de pacientes ou informações confidenciais do hospital.

Perda ou exclusão acidental de dados pessoais.

Senha possivelmente comprometida.

Entrega de documentos ao indivíduo não autorizado a receber.

Deixar computador desbloqueado ou ETICS logado, facilitando acesso indevido por outros.

Pessoa entrando em algum local indevido e acessando gavetas, armários sem autorização.

FUNCIONÁRIOS:

A segurança da informação é fundamental para proteger os dados dos pacientes e garantir a privacidade e a integridade das informações. Esta cartilha fornece orientações básicas para ajudar você a manter a segurança no ambiente hospitalar.

1. Proteção de Senhas

- Nunca compartilhe suas senhas: Senhas são pessoais e intransferíveis.
- Utilize senhas fortes: Combine letras maiúsculas, minúsculas, números e caracteres especiais.
- Troque suas senhas regularmente: Faça isso pelo menos a cada três meses.
- Não anote suas senhas em lugares visíveis: Use um gerenciador de senhas seguro.

2. Cuidado com E-mails e Links

- Verifique o remetente: Não abra e-mails de remetentes desconhecidos.
- Não clique em links suspeitos: Podem conter malware ou direcionar para sites de phishing.
- Não forneça informações pessoais via e-mail: Se necessário, confirme a solicitação por outro meio.

3. Segurança de Dispositivos

- Tranque seu computador quando não estiver usando: Utilize Ctrl + Alt + Del e selecione "Bloquear".
- Atualize seus softwares regularmente: Incluindo antivírus e sistemas operacionais.
- Não use dispositivos pessoais para trabalho: Utilize apenas dispositivos fornecidos pelo hospital.

4. Armazenamento e Compartilhamento de Dados

- Armazene informações sensíveis em locais seguros: Use armários trancados e sistemas de armazenamento criptografados.
- Compartilhe dados apenas com pessoas autorizadas: Certifique-se de que quem recebe as informações tem permissão para acessá-las.
- Use canais seguros para compartilhar informações: Evite o uso de e-mails pessoais ou dispositivos não autorizados.

5. Relate Incidentes de Segurança

- Qualquer incidente deve ser reportado imediatamente: Isso inclui perda de dispositivos, acessos não autorizados e e-mails de phishing.
- Informe à equipe de TI: Use os canais oficiais para reportar incidentes.

6. Política de Mesa Limpa

- Mantenha sua mesa organizada: Evite deixar documentos confidenciais expostos.
- Guarde documentos importantes: Use gavetas trancadas e áreas seguras.
- Descarte documentos de forma segura: Utilize trituradores de papel para documentos sensíveis.

7. Uso de Redes e Internet

- Acesse apenas sites confiáveis: Evite navegar em sites não relacionados ao trabalho.
- Não baixe software não autorizado: Todos os programas devem ser aprovados pelo departamento de TI.
- Cuidado com redes Wi-Fi públicas: Sempre use VPN ao acessar informações hospitalares fora do ambiente de trabalho.

8. Privacidade e Confidencialidade

- Respeite a privacidade dos pacientes: Não compartilhe informações médicas fora do ambiente de trabalho.
- Assine um termo de confidencialidade: Esteja ciente das responsabilidades legais sobre o uso e proteção de dados.
- Evite discussões sobre pacientes em áreas públicas: Mantenha conversas profissionais restritas a áreas privadas.

Seguir essas orientações ajuda a manter a segurança das informações e protege a privacidade dos pacientes e funcionários do hospital. Todos somos responsáveis por garantir um ambiente seguro e protegido.

Hospital Metropolitano Regional