DOM ORIONE
HOSPITAL

MANUAL DE BOAS PRÁTICAS LGPD

1ª EDIÇÃO - 2025

SOBRE O
HOSPITAL DOM ORIONE

MISSÃO

Prestar serviços de saúde humanizados, com qualidade, vivenciando o carisma de São Luís Orione.

VISÃO

Ser excelência na saúde para a população da região, de acordo com os princípios Orionitas.

VALORES

Ética Cristã, Segurança, Qualidade, Inovação e Sustentabilidade.

NEGÓCIO

Saúde de acordo com o Carisma de São Luís Orione.

DOM ORIONE
HOSPITAL

Expediente

Pe. Bruno Rodrigues
Diretor Presidente

Osvair Murilo da Cunha
Superintendente Executivo

Dr. Arnaldo Alves Nunes
Diretor Técnico Médico

Drª. Walide Wadih Salame
Diretora Técnica Adjunta

Mara Cristina
Gerente de Qualidade

PROJETO GRÁFICO E DIAGRAMAÇÃO
Evando Dias Rodrigues
Assistente de Comunicação e Marketing

MANUAL DE **BOAS PRÁTICAS**

OBJETIVO

Disseminar a cultura de conformidade e privacidade da LGPD no dia a dia do hospital, garantindo a proteção dos dados dos pacientes e a segurança das informações.

PÚBLICO-ALVO

Todos os profissionais do Hospital Dom Orione.

APRESENTAÇÃO

Este manual tem como objetivo fornecer orientações práticas e acessíveis sobre como aplicar os princípios da Lei Geral de Proteção de Dados (LGPD) nas atividades diárias no hospital. Ao seguir estas práticas, você contribui para a construção de um ambiente mais seguro, transparente e confiável para os pacientes, colaboradores e demais envolvidos.

O QUE É A **LGPD?**

LGPD é a sigla para Lei Geral de Proteção de Dados, a Lei nº 13.709/2018, que regulamenta a maneira pela qual os dados pessoais são utilizados por pessoas ou empresas, criando exigências para o seu tratamento, que inclui sua coleta, utilização, armazenamento e eliminação no meio físico e digital.

QUAL A SUA FINALIDADE?

A LGPD regulamenta o uso, proteção e transferência de dados pessoais no Brasil, visando proteger a liberdade, privacidade e individualidade das pessoas.

Diante do crescente compartilhamento de dados em diversas atividades (online e offline), a lei estabelece regras para garantir que as informações sejam tratadas de forma segura e ética.

CONCEITOS E DEFINIÇÕES

· **Dados pessoais:** Qualquer informação que possa levar à identificação de uma pessoa natural (titular), como: nome, endereço, e-mail, identidade, CPF, dados de localização (o GPS no celular), endereço de IP do computador e tantos outros.

· **Dados pessoais sensíveis:** Qualquer informação que possa causar impacto mais relevante na vida pessoal e/ou profissional, caso seja exposta ou compartilhada, como: dado de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde, à vida ou orientação sexual, dado genético ou biométrico.

· **Dados Anonimizados:** São aqueles relativos a uma pessoa natural, mas que passaram por tratamentos técnicos para garantir a desvinculação deles da pessoa titular. Os dados anonimizados não estão sujeitos à LGPD. No encobrimento de caracteres, um símbolo (como "*" ou "x") é usado para substituir caracteres relativos ao dado. Por exemplo, em uma tabela com números de telefone, pode-se optar por encobrir o número com "x" e manter apenas o código de área: (41) xxxx-xxxx.

ATORES DA **LGPD**

TITULAR

É pessoa natural a quem se referem os dados que serão tratados.

CONTROLADOR

É o responsável a quem competem as decisões referentes ao tratamento de dados pessoais.

OPERADOR

Pessoa ou empresa, que realiza o tratamento de dados pessoais em nome do controlador.

ENCARREGADO

Também conhecido como DPO - Data Protection Officer, é a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

ANPD

Autoridade Nacional de Proteção de Dados, é a responsável por zelar, implementar e fiscalizar o cumprimento da LGPD pelas Organizações.

TRATAMENTO DE **DADOS PESSOAIS**

A LGPD define "tratamento" de dados pessoais como qualquer operação realizada com essas informações. Isso significa que praticamente tudo que você faz com dados pessoais se enquadra nessa definição. Veja os principais tipos de tratamento:

Coleta: Reunir dados com uma finalidade específica.

Armazenamento: Guardar dados em sistemas e arquivos.

Classificação: Organizar dados seguindo algum critério.

Processamento: Organizar dados para gerar relatórios e análises.

Utilização: Usar os dados para alguma finalidade.

Acesso: Consultar informações do titular.

Modificação: Alterar os dados.

Transferência: Mover os dados para outro local ou para terceiros.

Arquivamento: Manter dados guardados, mesmo que não sejam mais usados ativamente.

Comunicação: Transmitir informações sobre como os dados são tratados.

Controle: Regular, determinar ou monitorar o que é feito com os dados.

Eliminação: Excluir ou destruir os dados.

BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS

A LGPD determina 10 hipóteses ou bases legais que devem justificar o tratamento de dados pessoais. Estas bases são fundamentais para garantir que a empresa esteja em conformidade e adequada à lei.

01 Consentimento do titular

02 Cumprimento de obrigação legal

03 Execução de políticas públicas

04 Realização de estudos por órgão de pesquisa

05 Execução de contratos ou procedimentos preliminares

06 Exercício regular de direitos

07 Proteção da vida ou incolumidade física

08 Tutela da saúde

09 Interesses legítimos do controlador ou terceiro

10 Proteção do crédito

PRINCÍPIOS **FUNDAMENTAIS**

A LGPD possui princípios fundamentais que servem como pilares que orientam toda a interpretação e aplicação da lei. Eles são a base para garantir que o tratamento de dados pessoais seja realizado de forma ética, responsável e transparente, protegendo os direitos dos titulares dos dados.

01 Finalidade
Especificada e informada explicitamente ao titular.

02 Adequação
à finalidade previamente acordada e divulgada

03 Necessidade
do tratamento, limitado ao uso de dados essenciais para alcançar a finalidade inicial

04 Acesso Livre
fácil e gratuito das pessoas à forma como seus dados são tratados

05 Qualidade dos dados
deixando-os exatos e atualizados, segundo a real necessidade no tratamento.

06 Transparência
ao titular, com informações claras e acessíveis sobre o tratamento e seus responsáveis.

07 Segurança
para coibir situações acidentais ou ilícitas como invasão, destruição, perda e difusão.

08 Prevenção
contra danos ao titular e a demais envolvidos

09 Não discriminação
ou seja, não permitir atos ilícitos ou abusivos

10 Responsabilização
do agente, obrigado a demonstrar a eficácia das medidas adotadas

CONSENTIMENTO NA LGPD: O QUE VOCÊ PRECISA SABER

Como Obter: O consentimento deve ser explícito (por escrito ou outro meio que demonstre a vontade do titular) e destacado de outras cláusulas.

Prova: É responsabilidade do controlador provar que obteve o consentimento corretamente.

Sem Vícios: O consentimento não pode ser obtido de forma enganosa ou sob pressão.

Finalidade Específica: O consentimento deve ser para finalidades claras e específicas, não genéricas (» para todos os fins»).

Revogável: O titular pode revogar o consentimento a qualquer momento, de forma fácil e gratuita.

Informar Mudanças: Se a forma de uso dos dados mudar, o titular deve ser informado a ter a chance de revogar o consentimento.

Direito do Titular: O titular tem o direito de autorizar, negar ou mudar de ideia sobre o uso de seus dados.

SANÇÕES E MULTAS

A LGPD estabelece normas rigorosas para o tratamento de dados pessoais, e o descumprimento dessas normas pode resultar em sanções significativas.

MULTAS:

Até 2% do faturamento anual da empresa.

OUTRAS SANÇÕES:

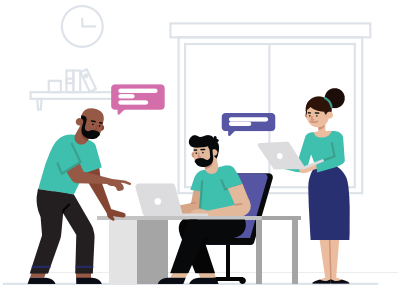
Advertência, com prazo para adoção de medidas corretivas.

Publicação da infração cometida.

Bloqueio ou *eliminação* dos dados pessoais irregulares.

Suspensão parcial ou total do funcionamento do banco de dados.

Proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados.



BOAS PRÁTICAS

1. Proteja suas senhas: Não compartilhe com ninguém e troque-as periodicamente. Exemplo: Use senhas com letras maiúsculas, minúsculas, números e símbolos, e troque a cada 3 meses.

2. Use a internet com responsabilidade: Não acesse sites suspeitos ou faça downloads ilegais. Exemplo: Evite sites de pirataria ou conteúdo inadequado na rede da empresa.

3. Cuidado com e-mails: Desconfie de mensagens estranhas e não clique em links ou baixe arquivos de remetentes desconhecidos. Exemplo: Se receber um e-mail pedindo para atualizar sua senha, verifique se o remetente é o oficial da empresa antes de clicar. Se, por engano, você clicar em algo suspeito, informe imediatamente o setor de TI.

4. Bloqueie a tela do computador: Sempre que se ausentar da sua mesa, mesmo que por um instante. Exemplo: Aperte "Windows + L" antes de ir ao banheiro ou pegar um café.

5. Proteja os dados em papel: Não deixe documentos com informações de clientes expostos e descarte-os corretamente. Exemplo: Picotar documentos com dados pessoais antes de jogar no lixo. E nunca utilizar o verso do papel para anotações ou novas impressões.

6. Seja discreto: Nunca comente informações confidenciais em lugares públicos ou com pessoas não autorizadas. Exemplo: Evite falar sobre clientes ou pacientes no elevador, refeitório, lanchonete, dentro e fora do ambiente de trabalho.

7. Priorize a Confidencialidade: É proibido o uso de celulares para tirar fotos ou gravar vídeos de pacientes, acompanhantes ou documentos com dados. Compartilhar essas imagens é violação da privacidade e da LGPD, sujeita a sanções. Em casos excepcionais, use apenas equipamentos e termos de consentimento da instituição.

BOAS PRÁTICAS

8. Seja transparente: Informe sempre ao cliente ou titular dos dados como você utilizará as informações que está coletando. Exemplo: Ao coletar o e-mail do cliente para enviar uma nota fiscal, informe que este será usado exclusivamente para esse fim.

9. Tenha consentimento: Obtenha o consentimento livre, informado e inequívoco do titular para o tratamento de dados, quando necessário.

10. Sigilo de Informações: Em hipótese alguma, forneça dados de pacientes ou colaboradores (nomes, informações médicas, etc.) a terceiros não autorizados, por qualquer meio. Lembre-se de que informações aparentemente simples podem ser utilizadas para fins ilícitos.

11. Respeite os direitos dos titulares: Atenda prontamente às solicitações dos titulares de dados, como acesso, correção, exclusão ou revogação do consentimento. Exemplo: Ao receber um pedido de exclusão ou alteração de dados, realize o procedimento. Se não houver justificativa legal para manter os dados, atenda ao pedido imediatamente.

12. Dados Sensíveis: Evite ao máximo coletar dados pessoais sensíveis (origem racial ou étnica, convicção religiosa, opinião política, de caráter religioso ou político, dado referente à saúde ou à vida sexual, etc). Em caso de necessidade, redobre os cuidados.

13. Use os sistemas da empresa: Evite criar planilhas ou documentos com dados de clientes em computadores pessoais ou em serviços de nuvem não autorizados.

14. Seja responsável: Entenda que a proteção de dados é responsabilidade de todos e que suas ações podem fazer a diferença. Exemplo: Se presenciar uma situação que possa comprometer a segurança dos dados, denuncie ao seu superior imediatamente.

15. Peça ajuda: Em caso de problemas relacionados à segurança da informação ou proteção de dados, procure os setores de Tecnologia da Informação (TI) ou Qualidade do HDO.

INFORMAÇÕES ÚTEIS

Para dúvidas, solicitações ou qualquer assunto relacionado à Lei Geral de Proteção de Dados (LGPD), entre em contato através do e-mail: lgpd@hospitalorione.com.br ou (63) 3411-8787 - Ramal 2238.

Este manual será revisado e atualizado periodicamente para garantir que esteja em conformidade com a legislação vigente e com as melhores práticas de proteção de dados.

DOM ORIONE
HOSPITAL

3411- 8787

www.hospitalorione.com.br
@hospitaldomorione

Rua Dom Orione, 100 - Centro
Araguaína - To