

CARTILHA LGPD

Pensar na segurança dos seus dados,
também é uma forma de cuidar de você.



 **MEDDI
& LGPD**
MAIS SEGURANÇA E MAIS CONFIANÇA.

GRUPO **MEDDI**
MEDICINA & SAÚDE

SOBRE ESSA CARTILHA

Com esta cartilha, o Grupo Meddi não pretende esgotar os temas e as discussões pertinentes à LGPD, mas apresentar as principais diretrizes como forma de conscientização alinhadas com as nossas Políticas de Segurança da Informação e Privacidade e Proteção de Dados (disponíveis na Plataforma Qualiex).

O nosso compromisso é sempre agir com transparência e responsabilidade no manuseio dos dados pessoais respeitando a privacidade de seus clientes, colaboradores, médicos, fornecedores, prestadores de serviços.



1. O QUE É LGPD?

Devido ao crescimento significativo da utilização de dados pessoais e conseqüentemente dos incidentes de vazamentos, surgiu a necessidade de regulamentações, objetivando que os dados sejam usados de forma responsável e a privacidade dos seus titulares seja protegida. Nesse sentido, foi criada a LGPD (Lei Geral de Proteção de Dados).

2. Objetivo da Lei:

Respeitar os direitos fundamentais das pessoas, protegendo a privacidade, intimidade e liberdade de expressão, e garantir transparência no uso de dados das pessoas físicas em quaisquer meios (físico ou digital).

3. Conceitos Fundamentais:

Titular: Pode ser qualquer pessoa física que tenha seus dados tratados. Cliente, colaborador, médico, fornecedor, prestador de serviço.

Tratamento de dados: É qualquer operação realizada com os dados pessoais, como por exemplo: coleta, acesso, compartilhamento, utilização, processamento, classificação, armazenamento, entre outros.

Dados Pessoais: São todas as informações que podem identificar uma pessoa direta ou indiretamente. Exemplos: nome, documentos pessoais, telefone, data de nascimento e endereço, e-mail, entre outros.

Dados Pessoais Sensíveis: São dados que podem revelar aspectos da intimidade de uma pessoa. Exemplos: religião, origem racial ou étnica, filiação à sindicato, dados referentes à saúde, vida sexual, dados genéticos e biométricos.

ANPD Autoridade Nacional de Proteção de Dados: Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.

4. Agentes de Tratamento

Controlador: Pessoa natural ou jurídica a quem compete as decisões quanto ao tratamento de dados pessoais, determinando as suas finalidades, condições e os meios de processamento.

Operador: Pessoa natural ou jurídica que realiza o tratamento dos dados em nome do controlador, sendo responsável por implementar os processos necessários para o cumprimento dos requisitos legais e de segurança

5. Encarregado de Dados (DPO)

Quem é o DPO?

É o profissional, indicado pelo controlador, responsável para cuidar da proteção de dados pessoais.

Quais as funções do DPO?

- # Aceitar reclamações e comunicações dos titulares de dados, prestar esclarecimentos e adotar providências;
- # Receber as comunicações da ANPD e adotar providências; (aqui cabe uma observação de que ele também deverá responder aos demais órgãos de fiscalização)
- # Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- # Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

6. Princípios

Para facilitar o reconhecimento de boas condutas e também das práticas que são inadequadas no dia a dia de uma instituição, destacam-se os 10 princípios que norteiam a LGPD e que devem ser respeitados:

Finalidade: O tratamento dos dados pessoais deve ser feito de acordo com propósitos legítimos, específicos, explícitos e informados ao titular.

Adequação: Os dados pessoais tratados devem ser compatíveis com a finalidade informada pela entidade.

Necessidade: Coletar somente os dados que são realmente necessários àquela utilização.

Livre acesso: A pessoa física titular dos dados tem o direito de consultar, de forma simples e gratuita, todos os dados que a entidade detenha a seu respeito.

Qualidade dos dados: Deve ser garantido aos titulares que as informações que a empresa tenha sobre eles sejam verdadeiras e atualizadas.

Transparência: Todas as informações passadas pela empresa, em todos os seus meios de comunicação, devem ser claras, precisas e verdadeiras.

Segurança: Medidas técnicas e administrativas utilizadas para proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas, de destruição, perda, alteração, comunicação ou difusão.

Prevenção: Medidas utilizadas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Não Discriminação: Os dados pessoais jamais podem ser usados para discriminar ou promover abusos contra os seus titulares.

Responsabilização e Prestação de Contas: Além do cumprimento integral da

lei, os agentes de tratamento devem comprovar que realizam todas as medidas necessárias, para demonstrarem a sua boa-fé e a sua diligência.

7. Direitos dos Titulares

Confirmação - Confirmar se existem dados.

Acesso - Acessar os dados que são tratados.

Correção - Corrigir os dados.

Anonimização, Bloqueio, Eliminação - Solicitar anonimização, bloqueio, ou eliminação dos dados.

Portabilidade - Solicitar portabilidade dos seus dados pessoais para outra organização fornecedora do produto ou serviço.

Revogação de Consentimento - Revogar o consentimento concedido anteriormente.

Informação sobre compartilhamento - Qual entidade pública ou privada os dados poderão ser compartilhados.

O titular pode exercer seus direitos através do Canal de Privacidade disponível no site do Grupo Meddi e/ou contato direto com o DPO.

<https://www.grupomeddi.com.br/index.html>

DPO: (75) 98142-8251

8. DICAS DE BOAS PRÁTICAS



Os documentos em papéis e mídias eletrônicas não devem permanecer sobre a mesa, devem ser armazenados em armários ou gavetas trancadas;



Anotações, recados e lembretes não devem ser deixados à mostra sobre a mesa ou colocados em paredes, divisórias ou monitor do computador;



Não guardar pastas com documentos sensíveis em prateleiras de fácil acesso;



Não imprimir documentos apenas para lê-los. Leia-os na tela do computador, se possível;



Não reaproveitar páginas já impressas e contendo informações pessoais e/ou confidenciais, devendo as mesmas ser descartadas;



Destruir os documentos impressos antes de jogá-los fora. Sempre que possível utilizar máquinas fragmentadoras;



Informações sensíveis ou confidenciais, quando impressas em local coletivo, devem ser retiradas da impressora imediatamente;



Cuidado com o descarte de dados pessoais que envolvem a operação (pulseiras de identificação, etiquetas, ordem de serviço, guia TISS...). Garantir que os documentos foram destruídos antes do descarte;



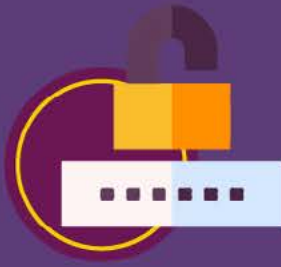
Não deixar os computadores logados caso precise se ausentar e ao final do expediente limpar a mesa, guardar os documentos, trancar gavetas e armários e desligar o computador;



Atenção com os resíduos biológicos e películas radiográficas, estes contêm dados sensíveis e precisam ser descartados de acordo com PGRSS (Plano de Gerenciamento de Resíduos dos Serviços de Saúde);



Nunca deixe crachá de identificação ou chaves em qualquer lugar, mantenha-as junto a você;



Não compartilhar a conta de acesso e senha com outro usuário, colaborador e/ou terceiro;



Não liberar resultados de exames sem a devida confirmação do titular dos dados;



Não utilizar celulares para produção de qualquer tipo de imagem, foto, vídeo, áudio relacionado ao ambiente corporativo do Grupo MEDDI sem a expressa autorização da organização;



As informações dos titulares de dados não devem ser discutidas ou expostas em nenhuma área pública, incluindo elevadores, corredores e refeitórios, especialmente junto com terceiros estranhos aos fluxos de trabalho;



Cuidado com o fornecimento de informações de pacientes por telefone ou aplicativo de mensagens;



Cuidado com o compartilhamento de dados pessoais através do aplicativo WhatsApp, anonimizar a informação sempre que possível, limpar histórico de conversa diariamente, garantir a segurança do aplicativo por meio de senhas e autenticação de dois fatores para mitigar o risco de vazamento de dados.

Cabe a cada um de nós o dever de proteger e salvaguardar os dados pessoais de seus respectivos titulares, é importante que esse cuidado esteja presente em todas as formas de acesso, como papel, qualquer meio eletrônico, verbal, telefônico, entre outros.

9. Governança

Os projetos, produtos e serviços a serem desenvolvidos devem nascer em conformidade aos requisitos da LGPD e ao programa de privacidade do Grupo Meddi. Processos que tratam dados pessoais e passarão por mudanças precisam envolver o DPO para garantir a continuidade da conformidade com a legislação vigente.

Fique atento a situações do dia-a-dia que podem representar impacto no cumprimento da LGPD. **Não hesite em procurar o DPO ou acessar o Canal de Denúncia.**

O objetivo do Canal de Denúncia é apurar situações de não conformidade com a Política de Segurança da Informação, principalmente situações onde dados sensíveis de pacientes, colaboradores ou parceiros correm o risco de serem acessados por pessoas não autorizadas e conseqüentemente passarem a apresentar riscos aos seus titulares.

O canal é destinado a colaboradores, fornecedores, clientes e terceiros para que comuniquem exclusivamente situações de prática suspeita ou não ética relacionadas à segurança da informação. É uma ferramenta importante para o Comitê Gestor de Segurança da Informação e Proteção de Dados – CGSIPD, grupo de trabalho multidisciplinar permanente, efetivado pela diretoria do Grupo MEDDI, que tem por finalidade tratar questões ligadas à Segurança da Informação e Proteção de Dados reduzindo os riscos para manter um ambiente de trabalho livre de irregularidades. Você não precisa se identificar.

DPO: dpo@meddi.com.br

Segurança da Informação: segurancati@meddi.com.br

Canal de denúncia:

https://app.protegon.com.br/#/external_incident_complaint/88802c9a

<https://www.grupomeddi.com.br/index.html>



MAIS SEGURANÇA E MAIS CONFIANÇA.

