CREFONO 2
Conselho Regional de Fonoaudiologia de São Paulo

# FONOAUDIOLOGIA COM A LGPD

Boas Práticas sobre a Lei Geral de Proteção de Dados (LGPD) para o Fonoaudiólogo

# APRESENTAÇÃO

LGPD

A Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) visa a **proteção de dados pessoais.**

A lei se aplica a todos, sejam pessoas ou empresas, e também inclui o uso de tecnologias digitais.

- Na área da **saúde**, muitos **dados** sensíveis são coletados durante o **atendimento.** Esses dados podem trazer algum tipo de exposição ao cliente, e, por isso, precisam ser devidamente protegidos.
- A LGPD faz com que seja importante rever **como** esses dados são **registrados** e **armazenados** nas clínicas.
- Não seguir as regras da LGPD pode resultar em penalidades sérias. Portanto, é fundamental **garantir** que todas as **práticas** estejam **de acordo com essa lei**.

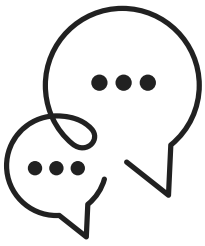
A LGPD (Lei 13.709/18), com vigência integral em 2020, objetiva a **proteção do uso dos dados pessoais** dos cidadãos, impondo **regras** sobre o **tratamento** desses **dados** pelas empresas.

# LGPD NA SAÚDE

Veja aqui como a LGPD impacta diretamente a sua rotina de trabalho, destacando a importância da privacidade e proteção de dados no seu dia a dia como profissional de saúde. Vamos descobrir como você pode se adequar às regulamentações da LGPD para garantir a segurança e confidencialidade das informações dos seus clientes, enquanto oferece a melhor qualidade de atendimento.

## Prontuário, Armazenamento e Backup de dados

- Obtenha o **consentimento** informado dos clientes antes de coletar qualquer dado pessoal.
- Colete apenas os dados **estritamente necessários** para o tratamento.
- Mantenha os prontuários **atualizados**, registrando todas as informações relevantes sobre o tratamento.
- Garanta que apenas **pessoas autorizadas** tenham acesso aos prontuários.
- Informe os clientes sobre seus direitos de acesso, retificação, exclusão e portabilidade de dados.
- Implemente **medidas de segurança**, como senhas e autenticação de dois fatores, para proteger os prontuários eletrônicos contra acessos não autorizados.
- Utilize **sistemas de armazenamento criptografado** e faça **backups** regularmente para também garantir a disponibilidade dos dados em caso de falhas técnicas ou desastres.
- Em caso de prontuários físicos, garanta que o local de armazenamento seja **restrito** e **trancado** com chave.
- Armazene os backups em locais seguros e garanta que sejam facilmente recuperáveis.
- Defina procedimentos adequados para a eliminação segura de dados pessoais quando não forem mais necessários, se atentando aos prazos legais de armazenamento.



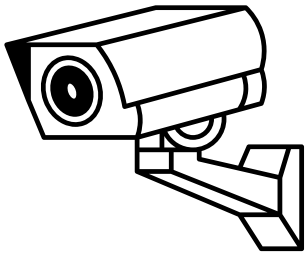
## Atendimento e Compartilhamento via Whatsapp

- Obtenha o **consentimento** prévio e informado do cliente para a coleta e compartilhamento de dados via WhatsApp.
- Certifique-se de que o cliente esteja ciente de como suas informações serão usadas e compartilhadas.
- Garanta que a **identidade** de ambas as partes seja verificada.
- Não compartilhe informações de clientes em grupos públicos ou com pessoas não autorizadas.
- Colete apenas os dados necessários para o atendimento.
- Evite solicitar informações excessivas e não relacionadas ao tratamento.
- Tanto o profissional quanto o cliente têm responsabilidades no compartilhamento seguro de dados.
- Os clientes devem estar cientes dos riscos e agir de maneira responsável ao enviar informações.
- Forneça orientações claras aos clientes sobre como usar o WhatsApp de forma segura ao compartilhar informações de saúde e lembre-os de evitar o envio de dados sensíveis em chats públicos.

# LGPD NA SAÚDE

## Compartilhamento com outros profissionais

- Obtenha o **consentimento** dos clientes (e dos responsáveis legais, se for o caso) antes de compartilhar qualquer informação com outros profissionais.
- Compartilhar informações somente quando for justificado pela necessidade de tratamento ou diagnóstico do cliente, e que sejam apenas informações mínimas necessárias para atender ao propósito específico do compartilhamento.
- Faça uso de **meios seguros de compartilhamento** de informações, como sistemas de saúde eletrônicos protegidos por senha ou criptografia de dados.
- Mantenha **registros** detalhados de qualquer compartilhamento de informações, incluindo datas, finalidades e destinatários.
- Limite o acesso às informações apenas aos profissionais autorizados que tenham uma necessidade legítima de acesso.



## Câmeras de Segurança

- Afixe **avisos visíveis** em áreas onde as câmeras de segurança estão em operação para informar as pessoas de que estão sendo gravadas. Sempre coloque a placa **visível** e **antes do acesso** ao cômodo da câmera.
- Garanta que as câmeras de segurança capturem apenas as áreas estritamente necessárias para a segurança, evitando a gravação de áreas privadas ou de tratamento.
- Estabeleça políticas que determinem por quanto tempo as gravações serão armazenadas e, em seguida, garantam que elas sejam excluídas após o período determinado.
- Limite o acesso às gravações de vídeo apenas a pessoas autorizadas.
- Implemente medidas de segurança para proteger as gravações de vídeo contra acesso não autorizado.
- Estabeleça procedimentos claros para o acesso às gravações em caso de incidentes, como invasões, furtos ou outros eventos que exijam investigação.

## Instruções sobre Crianças e Adolescentes

- Informações relacionadas a crianças e adolescentes merecem uma proteção especial devido à vulnerabilidade dessa faixa etária. O **consentimento dos pais ou responsáveis legais** é necessário para coletar e processar dados de crianças menores de idade. Isso se aplica mesmo que a criança ou adolescente tenha dado seu consentimento.
- Seja **transparente** com os pais ou responsáveis sobre **como** os dados da criança ou adolescente **serão coletados, usados e protegidos**. Explique claramente os objetivos da coleta de dados.
- Colete apenas informações necessárias para o atendimento. Evite coletar informações excessivas ou não relevantes para a finalidade pretendida.
- Os pais ou responsáveis têm o direito de **acessar** os dados coletados de seus filhos e de **retirar o consentimento** a qualquer momento.
- As informações que possam identificar crianças e adolescentes devem estar devidamente protegidas e não compartilhadas sem consentimento.

# LGPD NA SAÚDE

## Compartilhamento em Redes Sociais (Instagram, Youtube, etc)

- Certifique-se que em qualquer compartilhamento em redes sociais as informações referente a identificação do cliente seja **anonimizada** e a **reidentificação seja impossível**.
- Caso o cliente tenha dado o consentimento explicito que seja por escrito e no caso de criança e adolescente colete também a autorização do representante legal. **Eles devem ser informados sobre como seus dados serão usadas.**
- No uso de vídeos, fotos ou demais dados biométricos tenha certeza que o cliente está ciente de como as suas informações serão usadas.

- Certifique-se de que o compartilhamento em redes sociais tenha uma **finalidade legítima**, como educação, conscientização ou demonstração de casos de sucesso em tratamentos.
- Mantenha o **controle sobre os comentários** e interações nas postagens, garantindo que nenhum dado pessoal sensível seja compartilhado pelos clientes ou terceiros.
- Esteja preparado para remover ou desidentificar informações de clientes, conforme solicitado por eles, respeitando o direito ao esquecimento.
- Seja um exemplo responsável para outros profissionais ao compartilhar informações nas redes sociais, promovendo a proteção da privacidade do cliente.

## Casos Clínicos em Palestras

- Sempre **anoniminize** os dados pessoais que possam identificar algum cliente antes de incluir seus casos clínicos, fotos, ou qualquer informação identificável em palestras ou apresentações.
- Ao compartilhar casos clínicos, **remova qualquer informação que possa identificar diretamente o cliente**, como nomes, idades, datas de nascimento ou qualquer outra informação pessoal.
- Certifique-se de que os clientes (e seus representantes legais) tenham autorizado expressamente (de preferência por escrito) o uso de seus casos clínicos em apresentações e palestras. **Eles devem ser completamente informados sobre como suas informações serão usadas.** **Mantenha um registro dessas autorizações**.
- Garanta que o compartilhamento de informações seja estritamente para fins educacionais e que contribua para o avanço da prática fonoaudiológica.
- Compartilhe apenas as informações estritamente necessárias para atingir o objetivo educacional da palestra. **Evite detalhes excessivos**.
- Ao exibir fotos ou vídeos de clientes, **obtenha permissão específica para cada mídia compartilhada** e **limite a exposição a características físicas ou identificáveis**.
- Utilize configurações de privacidade em suas apresentações, restrinja o acesso a pessoal autorizado e evite compartilhamento público.

# BASES LEGAIS DA LGPD

As bases legais da LGPD são hipóteses que autorizam o tratamento de dados. A LGPD prevê 10 bases legais que não tem dependência ou preponderância entre si. No caso de tratamento de dados, pode-se escolher a(s) base(s) legal(is) que achar mais adequada para si. São elas:


Consentimento


Cumprimento da Obrigação Legal


Execução de Políticas Públicas


Estudos por Órgão de Pesquisa


Execução de Contrato/ Diligências Pré contratuais


Exercício Regular de Direitos


Proteção da Vida


Tutela da Saúde


Interesses Legítimos do Controlador/ Terceiro


Proteção ao Crédito

Na área da saúde, geralmente, se utilizam principalmente as seguintes bases legais:

## Consentimento pelo titular

O consentimento fornecido pelo titular deve conter **manifestação livre** e inequívoca que **concorda com o tratamento de seus dados pessoais** e deve ter uma **finalidade determinada**.

Ex: Quando o cliente concede dados para ser atendido por profissional da saúde.

## Cumprimento de Obrigação Legal

Cabe essa hipótese de tratamento quando uma legislação em vigor autoriza e/ou define requisitos para **cumprimento da obrigação legal**.

Ex: Quando o profissional tem por obrigação registrar, em prontuário físico e ou eletrônico, todos os atendimentos e procedimentos fonoaudiológicos, bem como faltas justificadas ou não, e desistência.

## ATENÇÃO:

De acordo com a ANPD, o tratamento de dados pessoais de **crianças** e **adolescentes** pode ser realizado com base nas hipóteses legais previstas na LGPD, como nos casos de **consentimento fornecido pelo titular e seus representantes legais**, de cumprimento de **obrigação legal**, de **proteção à vida** ou de atendimento a **interesse legítimo** do controlador.

Em qualquer situação, **o melhor interesse da criança e do adolescente deve prevalecer**, exigindo avaliação cautelosa por parte do profissional.

# COLETA DE DADOS:
## DADO PESSOAL / DADO PESSOAL SENSÍVEL

### DADO PESSOAL

É toda e **qualquer informação que identifique ou possa identificar uma pessoa natural**, podendo incluir informações disponíveis sob qualquer forma: papel, texto, fotos, gráficos, vídeo, áudio, ou qualquer outro meio que leve a identificação do indivíduo de modo direto ou indireto, como: nome, número de identificação, dados de localização, endereço, telefone, matrícula, etc.

### DADO PESSOAL SENSÍVEL

São os dados que podem de alguma forma discriminar o Titular, que revelem origem étnica ou raça, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, **dados referentes à saúde** ou à vida sexual, dados genéticos ou biométricos.

**Observação:** Informações como dados do cartão de crédito ou salário, por exemplo, não são consideradas sensíveis perante à LGPD.

### ATENÇÃO:

Embora os dados coletados pelos profissionais de saúde sejam fundamentados em uma base legal, é crucial avaliar quais informações dos clientes são essenciais para que os profissionais minimizem a coleta de dados e não se comprometam com dados excessivos.

# PRAZOS DE RETENÇÃO DE DADOS

Ainda que a possibilidade de tratamento venha pelo **consentimento**, essa **autorização** não dura para sempre. Deverá ser respeitado ***prazo legal*** ou ***pactuado*** com o próprio titular.

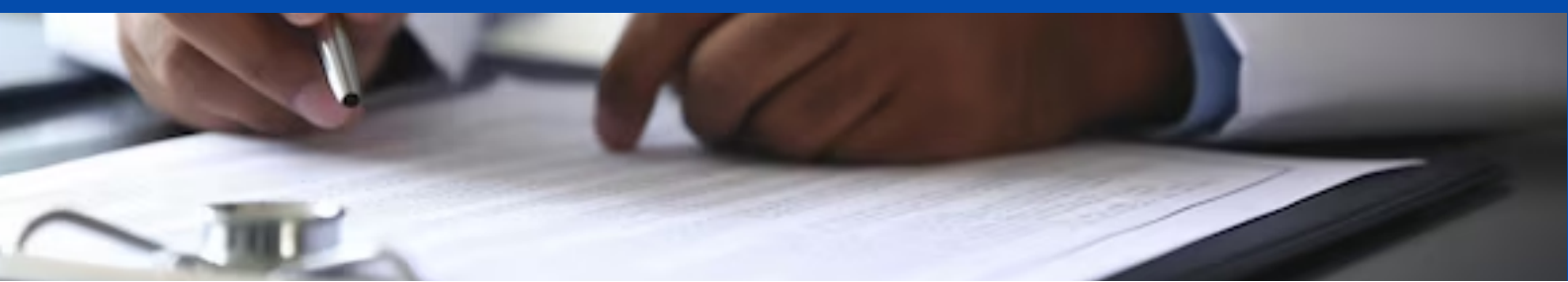
O tratamento dos dados pessoais **deve** ser **terminado** quando:

- A finalidade for alcançada;
- Os dados tratados não forem mais necessários para aquela finalidade;
- O período de tratamento acordado com o titular se encerrar;
- Quando o titular solicitar.

Mas ATENÇÃO: nem sempre os dados devem ser descartados.

Um exemplo claro é a conservação de dados em **prontuários**.
De acordo com a Lei nº 13.787/2018, o **período mínimo** de retenção de prontuários em formato físico ou digitalizado **é de 20 anos.**

É importante destacar que, mesmo se o titular solicitar a eliminação dos dados contidos nos prontuários, o profissional de fonoaudiologia pode, em certos casos, recusar essa solicitação, respaldado pelo artigo 16, inciso I, da Lei Geral de Proteção de Dados.



# CICLO DE VIDA

Os dados coletados pelo Conselho e seus associados devem ter uma **finalidade específica**. O ciclo de vida dessas informações começa com a **coleta de dados pessoais**, sejam eles sensíveis ou não. Esse ciclo vai **desde o tratamento inicial até a eliminação**, que pode ocorrer a pedido do titular dos dados, como parte de uma sanção ou no término do tratamento pelo detentor.

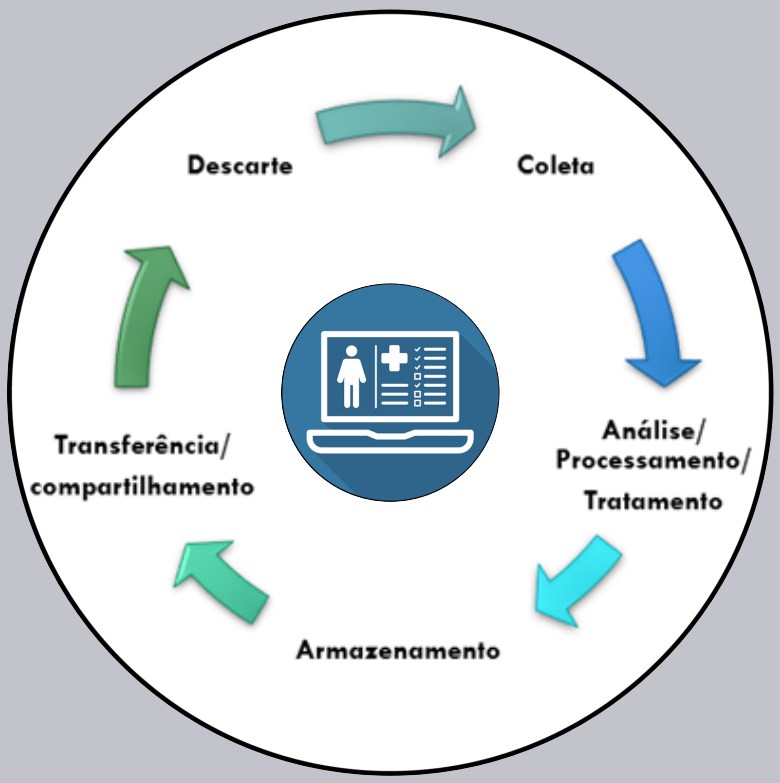
**Coleta:** Obtendo dados pessoais/sensíveis dos titulares de dados.

**Análise de Processamento:** Todas as operações que envolvem uso, processamento, avaliação, ou controle dos dados.

**Armazenamento:** Manter dados em local seguro para garantir a sua integridade e segurança.

**Transferência/Compartilhamento:** Qualquer operação com terceiros ou administração pública que envolve dados.

**Descarte:** Apagar ou eliminar dados, incluindo ativos organizacionais quando necessário.




## DIREITOS DO TITULAR DE DADOS

LGPD - Art. 18

# Orientações para Profissionais de Fonoaudiologia sobre o **Direito de Portabilidade de Dados**

A Lei Geral de Proteção de Dados (LGPD) estabelece importantes direitos para os indivíduos, conhecidos como titulares de dados, com relação às suas informações pessoais. Entre esses direitos, destaca-se o direito de portabilidade de dados, que **permite aos clientes a transferência segura de suas informações** de um controlador de dados para outro. Aqui estão algumas orientações sobre como esse direito se aplica à prática da fonoaudiologia:

O **direito de portabilidade** de dados permite que os clientes solicitem e recebam suas informações pessoais de um fonoaudiólogo e as transmitam a outro profissional de saúde, garantindo a interoperabilidade entre serviços de saúde.

**Atendimento Contínuo:** Este direito é particularmente relevante na área da fonoaudiologia. Imagine que um cliente deseje buscar uma segunda opinião ou continuar seu tratamento com outro fonoaudiólogo. Com o direito de portabilidade, eles podem solicitar a transferência de todos os dados relacionados ao seu tratamento, como registros de avaliações, diagnósticos e histórico de tratamento.

## Como Cumprir com o Direito de Portabilidade:

**Fornecimento de Dados Estruturados:** Ao receber uma solicitação de portabilidade de dados, **forneça todas as informações pessoais do cliente de forma estruturada e legível**. Isso deve ser feito em um formato que possa ser facilmente transmitido a outro controlador de dados, como outro fonoaudiólogo ou profissional de saúde.

## Segurança e Privacidade dos Dados:

**Proteção Rigorosa:** Certifique-se de que a segurança e a privacidade dos dados do cliente sejam rigorosamente mantidas ao cumprir com o direito de portabilidade. **Adote medidas apropriadas para proteger essas informações pessoais**, garantindo que elas não sejam divulgadas a terceiros não autorizados.

## Benefícios para o Cliente e para a Profissão:

**Cumprimento Legal:** O cumprimento adequado do direito de portabilidade fortalece a conformidade com a LGPD, demonstrando o **compromisso** do fonoaudiólogo com a privacidade e os direitos dos clientes.

A **segurança** e a **confidencialidade** das informações são fundamentais na prática da Fonoaudiologia e são uma parte essencial da conformidade com a **Lei Geral de Proteção de Dados (LGPD)**.

**1. Armazenamento Seguro:** Certifique-se de armazenar os dados dos clientes em locais seguros, seja em formato físico ou digital. Utilize armários trancados, pastas protegidas por senha e sistemas de segurança robustos para garantir que somente pessoas autorizadas tenham acesso a essas informações.

**2. Acesso Controlado:** Limite o acesso às informações dos clientes apenas a membros da equipe de saúde diretamente envolvidos no tratamento. Garanta que cada profissional tenha acesso apenas às informações necessárias para cumprir suas funções.

**3. Criptografia de Dados:** Se você lida com dados eletrônicos, utilize a criptografia para proteger as informações sensíveis dos clientes durante a transmissão e o armazenamento. Isso ajuda a evitar o acesso não autorizado.

**4. Treinamento da Equipe:** Ofereça treinamento regular sobre proteção de dados a todos os membros da equipe. Eles devem estar cientes das obrigações legais, das políticas internas e das melhores práticas para manter as informações dos clientes seguras.

**5. Consentimento Informado:** Certifique-se de obter o consentimento informado dos clientes para coletar, processar e armazenar seus dados. Explique claramente como as informações serão usadas e compartilhadas.

**6. Monitoramento de Acessos:** Implemente sistemas de monitoramento para rastrear o acesso aos registros dos clientes. Isso pode ajudar a identificar e resolver qualquer acesso não autorizado.

**7. Backup de Dados:** Faça backups regulares de todas as informações dos clientes. Isso garantirá que os dados estejam protegidos contra perdas acidentais, como falhas de hardware.

**8. Atualizações de Segurança:** Mantenha seus sistemas e software atualizados com as últimas correções de segurança. Isso ajuda a proteger contra ameaças cibernéticas.

**9. Plano de Resposta a Incidentes:** Desenvolva um plano de resposta a incidentes que descreva como lidar com vazamentos de dados ou violações de segurança, caso ocorram. A LGPD exige que esses incidentes sejam relatados às autoridades e aos titulares dos dados.

info@fonosp.org.br

www.fonosp.org.br/

instagram: @crefono2

CREFONO 2
Conselho Regional de Fonoaudiologia de São Paulo

Esta cartilha foi publicada pelo CREFONO2 e é de autoria da empresa 4D SOLUÇÕES.