PROTEÇÃO DE DADOS NA SAÚDE

BOAS PRÁTICAS PARA CONSULTÓRIOS, CLÍNICAS E PROFISSIONAIS AUTÔNOMOS DA ÁREA DA SAÚDE

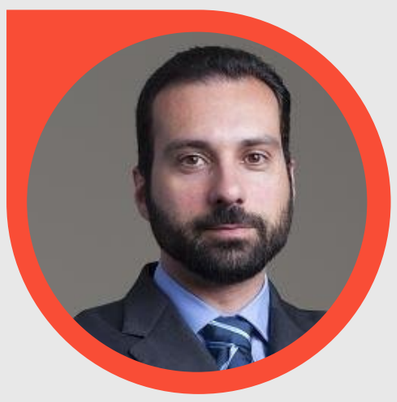
LAB next law academy

EXPEDIENTE

AUTORES

André Gonçalves

ADVOGADO EM PROTEÇÃO DE DADOS PESSOAIS, RIO DE JANEIRO - RJ



Lawrence King

ADVOGADO EM PROTEÇÃO DE DADOS PESSOAIS, RIO DE JANEIRO - RJ

Dyemülly Pegos

ADVOGADA EM PROTEÇÃO DE DADOS PESSOAIS, CURITIBA - PR

Lígia Lage

ADVOGADA EM PROTEÇÃO DE DADOS PESSOAIS, BELO HORIZONTE - MG

Eduardo Maroso

ANALISTA DE NEGÓCIOS E PROTEÇÃO DE DADOS PESSOAIS FLORIANÓPOLIS - SC

Luíza Patusco

ADVOGADA EM PROTEÇÃO DE DADOS PESSOAIS E STARTUPS, BELO HORIZONTE - MG

COORDENAÇÃO

Viviane Maldonado

DATA PROTECTION EXPERT, SÃO PAULO - SP

nextlaw academy

DESIGN VISUAL Dyemülly Pegos

REVISÃO TEXTUAL Luíza Patusco

DESENHOS MANUAIS Lígia Lage

SUMÁRIO

6 ALGUMAS SITUAÇÕES DE TRATAMENTO DE DADOS. O QUE FAZER?

7 COMO A LGPD AFETA O MEU CONSULTÓRIO?

8 COMO POSSO LEGITIMAR O TRATAMENTO DE DADOS PESSOAIS ?

9 QUAIS SÃO OS DIREITOS DOS TITULARES?

10 O QUE É UM AVISO DE PRIVACIDADE E POLITICA DE COOKIES?

O QUE É LGPD?

A Lei Geral de Proteção de Dados Pessoais - LGPD dispõe exclusivamente sobre o tratamento de dados pessoais de pessoa natural, seja por meios físicos ou digitais.

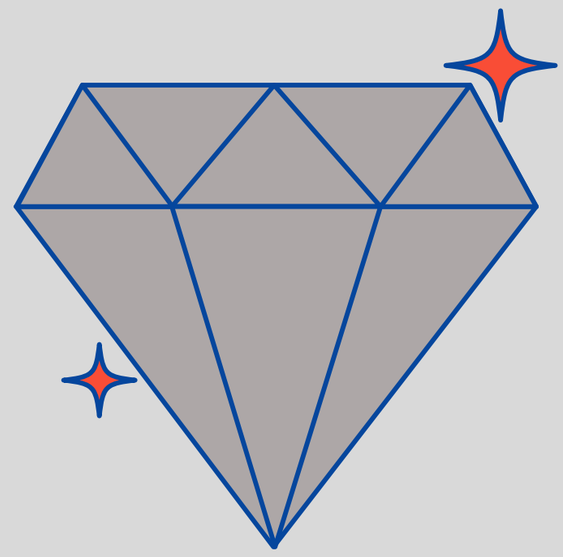
O intuito da lei é proteger os direitos fundamentais de liberdade, privacidade e personalidade de qualquer indivíduo.

QUEM DEVE CUMPRIR?

A lei deverá ser cumprida por entidades públicas e privadas (independentemente do seu porte) e por pessoas físicas que tratem dados pessoais com finalidade econômica.

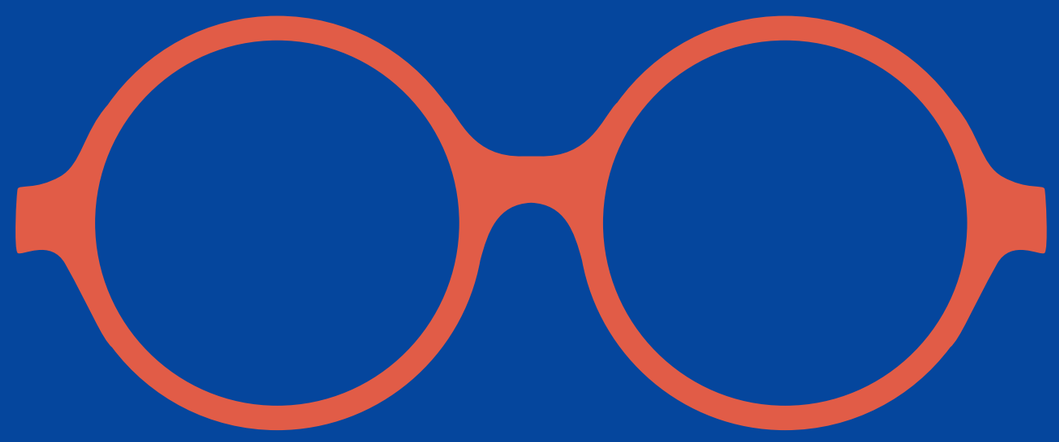
E A IMPORTÂNCIA?

Dados pessoais são ativos extremamente valiosos para as empresas. A regulação do tratamento permite que elas utilizem dados pessoais respeitando a privacidade do ser humano.

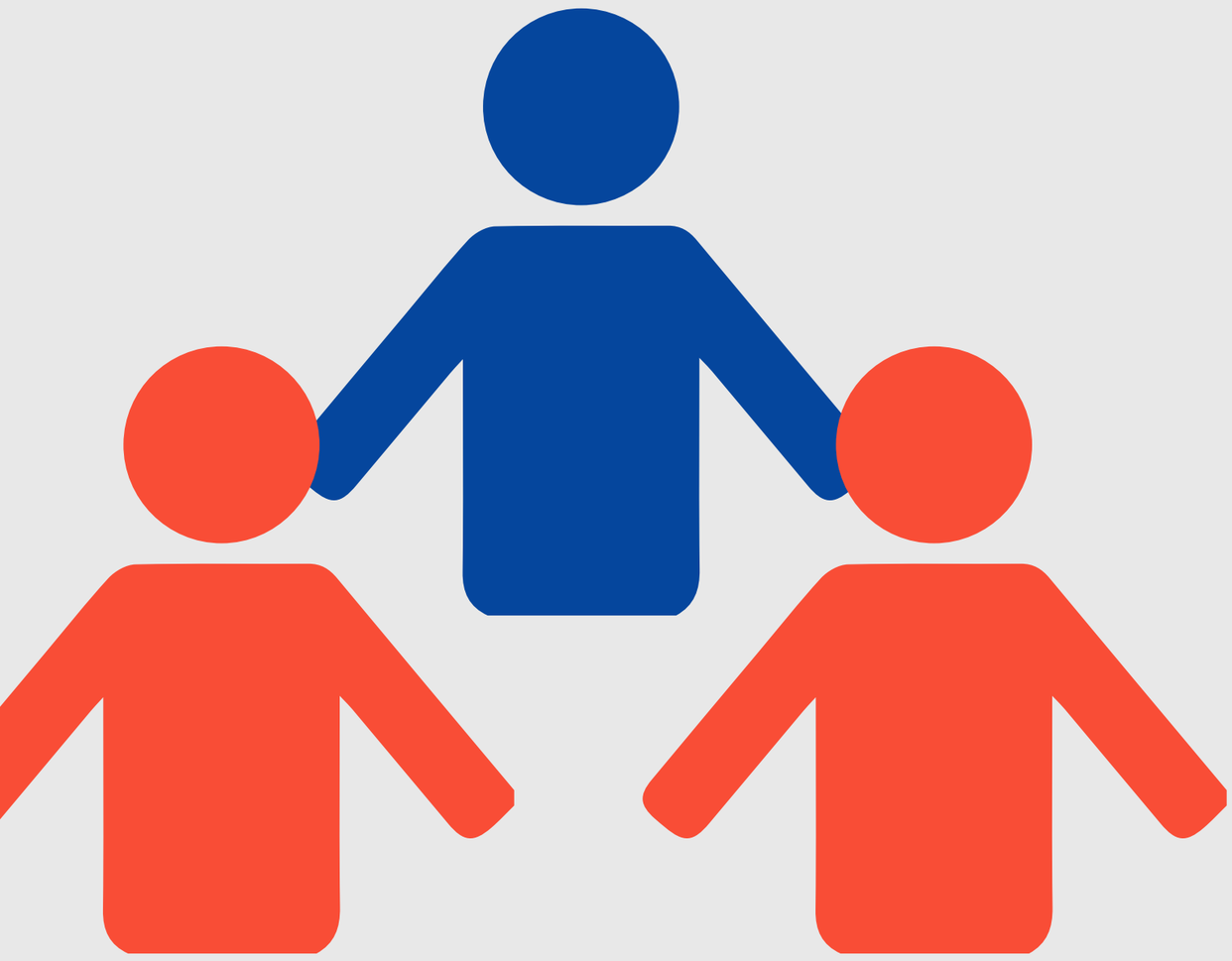


Empresas adequadas à LGPD possuem vantagem competitiva em relação às empresas que não estão em conformidade com a lei.

MAS O QUE É DADO PESSOAL?



É qualquer informação que possa identificar alguém de forma direta ou indireta.



QUEM É O TITULAR DOS DADOS PESSOAIS?

É a própria pessoa natural/física, ou seja, o indivíduo a quem os dados pessoais se referem.

Exemplo: o paciente e/ou colaborador do consultório odontológico.

QUEM CONTROLA E OPERA DADOS?

O **controlador** é a pessoa física ou jurídica que decide a forma como os dados pessoais serão tratados.

Exemplo: O dentista (profissional liberal) ou o consultório odontológico (pessoa jurídica) que coleta os dados de seus pacientes e define o que fará com eles.

O **operador** é a pessoa física ou jurídica que trata os dados dos titulares a partir das ordens recebidas pelo controlador.

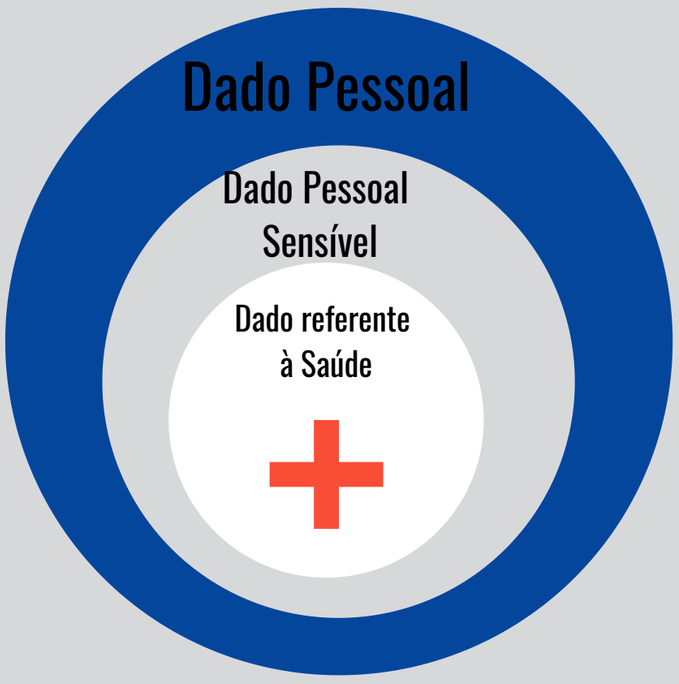
Exemplo: O laboratório que recebeu material para realização de uma biópsia.

Quando você escutar alguém falando em **agentes de tratamento**, normalmente estarão se referindo ao controlador e operador.

E O QUE É O TRATAMENTO DE DADOS?

É tudo que o controlador e/ou o operador fazem com o dado pessoal do titular desde a sua coleta até a sua eliminação.

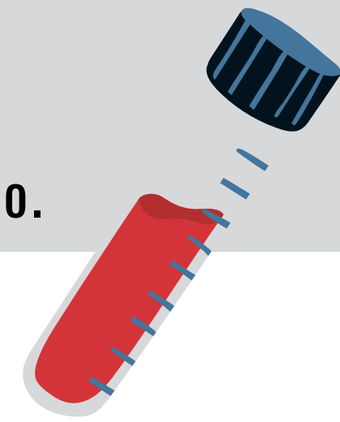
Exemplo: Quando um paciente (titular) vai até um consultório odontológico (controlador), primeiramente preenche-se uma ficha de cadastro. Neste momento são coletados dados cadastrais desse paciente, além de outras informações, como: motivo da consulta, se existe alergia a algum medicamento entre outras. Geralmente, tudo isso fica armazenado no consultório. Como o armazenamento é atividade de tratamento de dados pessoais, muitos deles sensíveis, é muito importante observar todos os aspectos da lei.

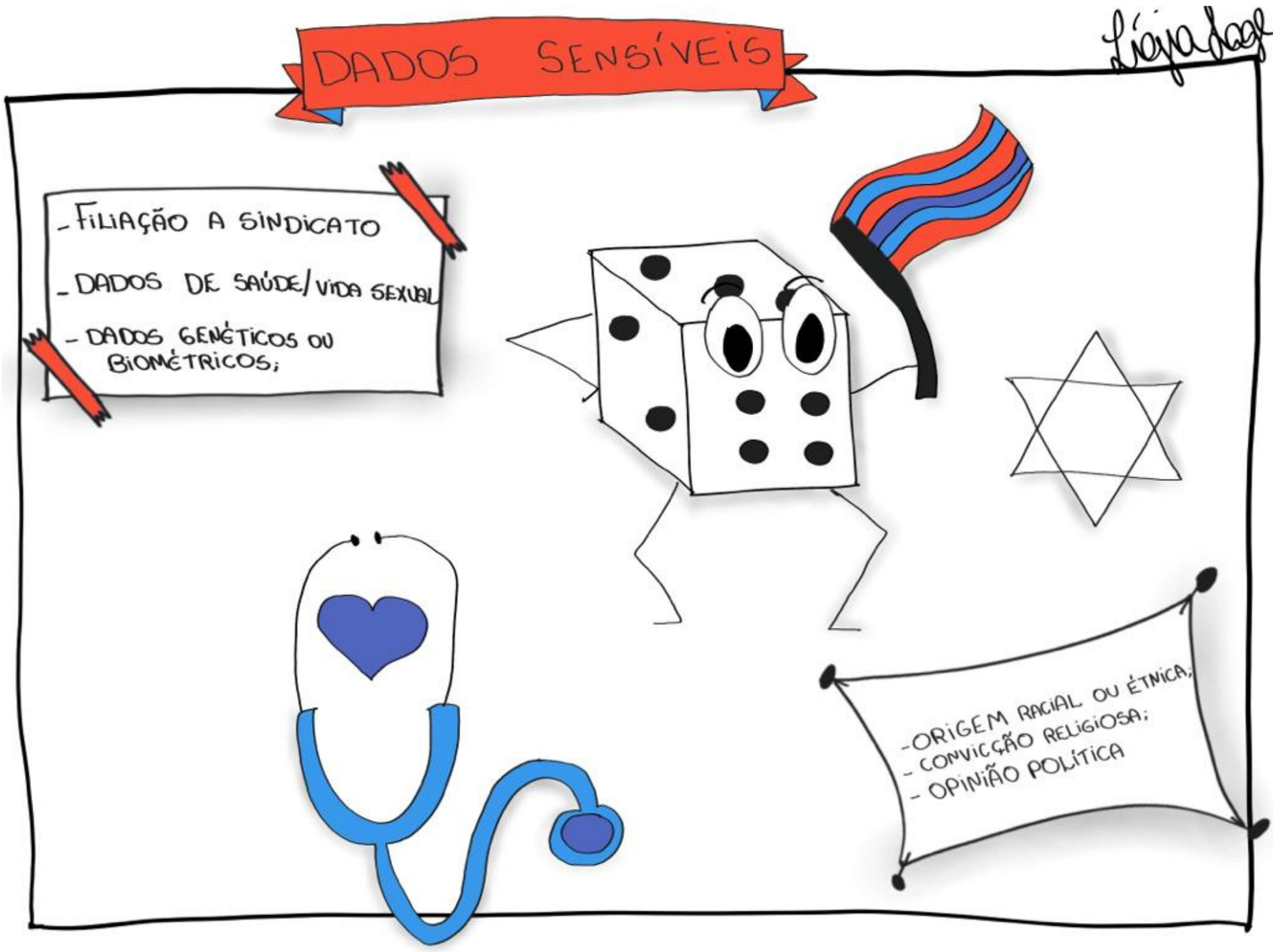


O QUE SÃO DADOS SENSÍVEIS?

São dados pessoais sobre a origem racial ou étnica de alguém, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Exemplo: Dados médicos do paciente, tipo sanguíneo.





ATENÇÃO: Um dado pessoal sensível é um dado pessoal, porém nem todos os dados pessoais serão sensíveis.

QUAIS SÃO OS IMPACTOS GERAIS DA LEI NA ÁREA DA SAÚDE?

O setor da saúde por si só já preza pelo sigilo e confidencialidade.
As regras estabelecidas na LGPD devem ser estritamente observadas sempre que dados pessoais forem tratados, sejam eles de pacientes, colaboradores (profissionais da saúde, técnicos, administrativos), visitantes, fornecedores e/ou terceirizados.

ATENÇÃO: Observar a lei do prontuário eletrônico juntamente com a LGPD.

E O QUE A LEI PROÍBE?

O compartilhamento de dados pessoais para outras finalidades.

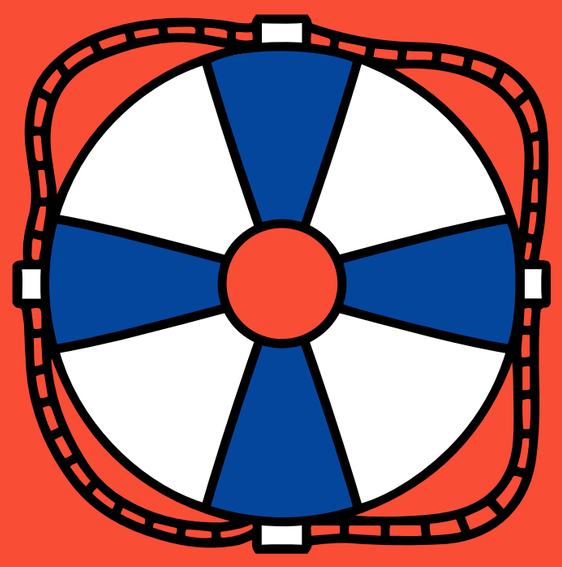
A lei veda expressamente a comunicação ou o uso compartilhado de dados pessoais sensíveis referentes à saude com o objetivo de obter vantagem econômica, exceto situações específicas.

As situações específicas são: o compartilhamento quando a finalidade é a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços de diagnóstico e terapia, em benefício dos interesses do titular.

O QUE É PRECISO DEFINIR ANTES DE TRATAR DADOS PESSOAIS?

FINALIDADE

Deve existir uma finalidade específica e legítima para o tratamento de cada dado pessoal.
Se não existir uma justificativa para a utilização de um dado pessoal, ele não deve ser tratado.



NECESSIDADE

Apenas os dados pessoais necessários para atingir a finalidade estabelecida devem ser coletados e utilizados.
Um dado pessoal não pode ser recolhido sob a hipótese de "quem sabe um dia será necessário".

ADEQUAÇÃO

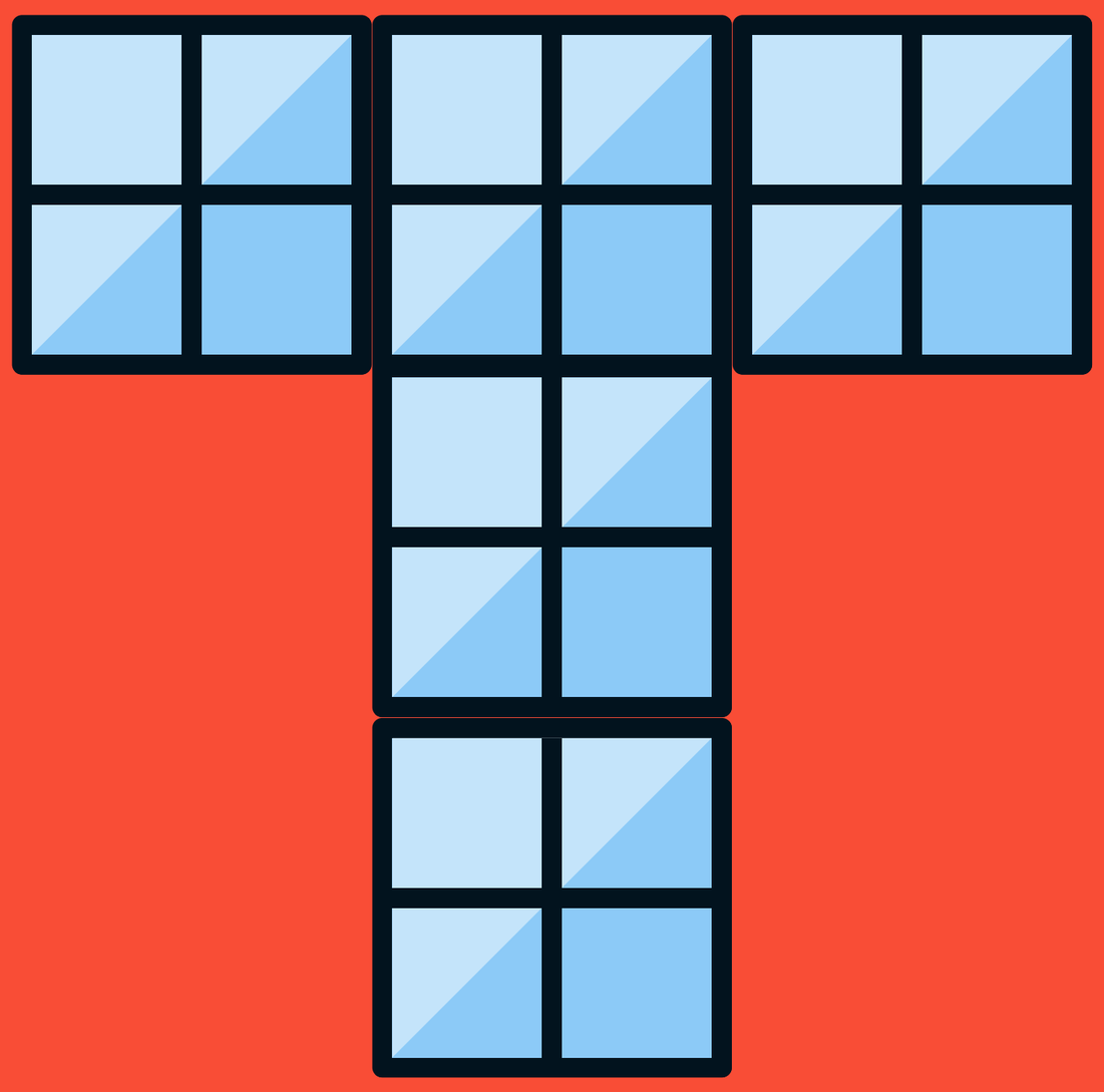
Os dados pessoais devem ser relevantes e adequados para atingir a finalidade fixada.

Exemplo: é necessário ou adequado saber a convicção religiosa de um paciente para fins de um atendimento ambulatorial? A resposta seria NÃO.
Mas e se o atendimento for cirúrgico? (há religiões que proíbem a transfusão de sangue).

O profissional ou a entidade de saúde deverá:

- ter conhecimento da finalidade da coleta dos dados;
- definir os dados pessoais necessários para essa finalidade.

Observação: Os profissionais ou entidades de saúde que tratem dados a pedido da operadora de plano de saúde devem observar as intruções de tratamento.



TRANSPARÊNCIA

O titular dos dados pessoais deve ser informado de forma clara e ter o acesso garantido às informações sobre os tratamentos realizados com seus dados pessoais, bem como sobre quem executa tais tratamentos.

Por isso é necessário criar procedimentos e documentos que permitam ao titular visualizar e entender quais são esses dados tratados, como e por quem estão sendo tratados.

A boa prática estabelece que, sempre que possível o titular deve ser informado no momento da coleta, porém, no setor da saúde, isso nem sempre será possível.

Exemplo: O responsável levando uma criança à emergência, possivelmente, não quer perder tempo na entrada do pronto socorro. Contudo, assim que possível, o responsável e a criança devem ter acesso à toda informação sobre os tratamentos de dados pessoais.

SEGURANÇA

É necessário implementar medidas reais de segurança e planos de contingência em caso de incidentes, como vazamentos ou perda de dados.

Todo material com dados pessoais deve estar sob controle e só pode ser acessado, visualizado, copiado, modificado ou destruído por quem tenha autorização para tanto.

O titular dos dados deverá ser informado quanto ao necessário compartilhamento de seus dados aos operadores.

ALGUMAS SITUAÇÕES DE TRATAMENTO DE DADOS. O QUE FAZER?

Quando um paciente recebe um formulário em papel na recepção de um consultório, qual será o destino deste documento após seu preenchimento? Quem terá acesso? Ele será digitalizado? Após a digitalização o formulário em papel será destruído?

Ao digitalizar documentos que contenham dados de saúde, antes de descartá-los é necessário triturá-los.

Caso a clínica ou hospital possuam computadores com acesso aos dados dos pacientes em diferentes salas e consultórios, há proteção por senha em cada terminal? Os computadores possuem programa antivírus atualizado? A rede é segura e protegida?

ATENÇÃO: Lembre-se que, se na mesa da recepção existir uma agenda em papel aberta com o nome e hora de atendimento de pacientes, há uma falha de segurança.

Ao contratar um provedor de plataforma de gerenciamento na nuvem, o profissional da saúde ou entidade não se exime de cumprir com os requisitos da LGPD e segue responsável pela segurança dos dados pessoais.

Então, é muito importante que se exija do provedor garantias de que ele cumpra com as normas da LGPD. Normalmente essas garantias deverão estar refletidas no contrato de serviços.

E se os dados pessoais forem armazenados fora do Brasil?

Neste caso, estaremos diante de uma transferência internacional de dados, que é regulada pela LGPD e só é permitida em casos específicos.

COMO A LGPD AFETA O MEU CONSULTÓRIO?

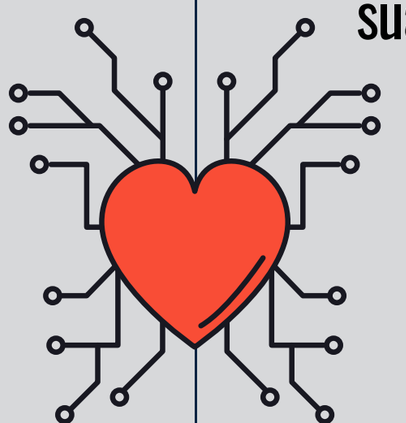
A LGPD afeta os consultórios em vários pontos:

- Coleta e tratamento de dados dos pacientes, clientes e funcionários
- Finalidade de dados tratados
- Necessidade dos dados tratados
- Segurança da informação
- Medidas de prevenção

Situações exemplificativas:

1. Profissionais de saúde que dividem o mesmo espaço e secretária necessitam redobrar os cuidados e se atentarem às medidas para mitigar a ocorrência de incidentes de segurança relacionados, por exemplo, ao acesso dos dados tratados.

2. Mesmo não se tratando de espaço compartilhado, os profissionais e funcionários devem ter restrições aos acessos de dados armazenados, acessando apenas dados estritamente necessários para o exercício de suas atividades.



E COMO EU POSSO LEGITIMAR O TRATAMENTO DE DADOS PESSOAIS EM MEU CONSULTÓRIO?

Através do que chamamos de bases legais.

QUAIS SÃO AS BASES LEGAIS

No caso de tratamento de dados sensíveis são:

CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA PELO CONTROLADOR

Quando o consultório deve enviar à Receita Federal os dados dos pacientes para os quais ele emitiu nota fiscal de prestação de serviço, para fins contábeis, por exemplo.

EXERCÍCIO REGULAR DE DIREITO EM PROCESSO

Quando o consultório e/ou profissional da saúde precisar se defender em processo judicial, administrativo, arbitral ou ajuizar ação.

PROTEÇÃO DA VIDA E SAÚDE DO TITULAR OU DE TERCEIROS

Quando ocorre um acidente, o titular se encontra inconsciente e os socorristas necessitam verificar seus documentos pessoais para informar a família, por exemplo.

TUTELA DA SAÚDE

É destinada especificamente para procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

GARANTIA DE PREVENÇÃO À FRAUDE E À SEGURANÇA DO TITULAR

Essa base legal é utilizada para autenticação de cadastro em sistemas eletrônicos. Algumas operadoras de saúde exigem autenticação biométrica para liberação de consultas, por exemplo.

CONSENTIMENTO

Autorização livre, informada e inequívoca do titular, concordando com o tratamento de dados para finalidade específica.

ATENÇÃO: O consentimento só deve ser utilizado no caso de que alguma das bases legais anteriormente citadas não se aplique ao caso concreto.

QUAIS SÃO OS DIREITOS DOS TITULARES?

(As solicitações dos titulares deverão ser processadas e o agente de tratamento verifica se pode ou não atender)

1. Confirmação do tratamento e acesso aos dados pessoais
2. Retificação dos dados pessoais
3. Anonimização
4. Bloqueio ou eliminação de dados pessoais
5. Informação de compartilhamento de dados
6. Informações para não fornecer o consentimento

7. Revogação do consentimento
8. Portabilidade de dados pessoais
9. Petição à ANPD
10. Não discriminação
11. Revisão de decisões automatizadas
12. Oposição ao tratamento

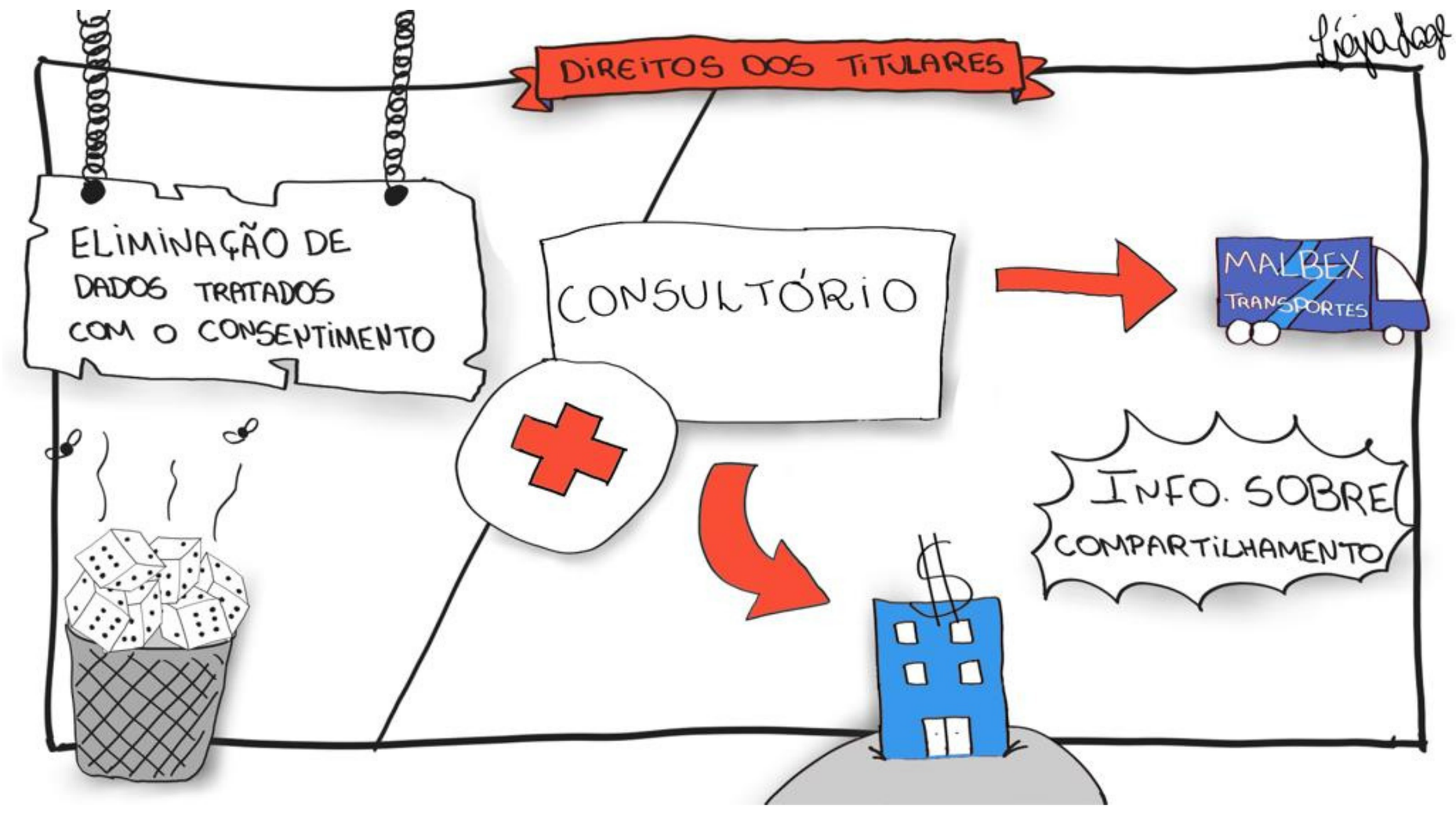
1.Confirmação do tratamento e acesso aos dados pessoais: direito de obter do controlador a confirmação e acesso sobre a existência de tratamento dos seus dados pessoais, através de informações claras sobre a sua origem, finalidade do tratamento ou inexistência de registro.

2.Retificação dos dados pessoais: direito de requerer a correção de dados incompletos, inexatos ou desatualizados. Você deverá providenciar a correção e comunicar aos agentes de tratamento com quem tenha compartilhado os dados para que realizem imediatamente o mesmo procedimento.

3.Anonimização: procedimento que impede a identificação do titular aos seus dados pessoais que estão dentro do banco de dados do seu consultório.

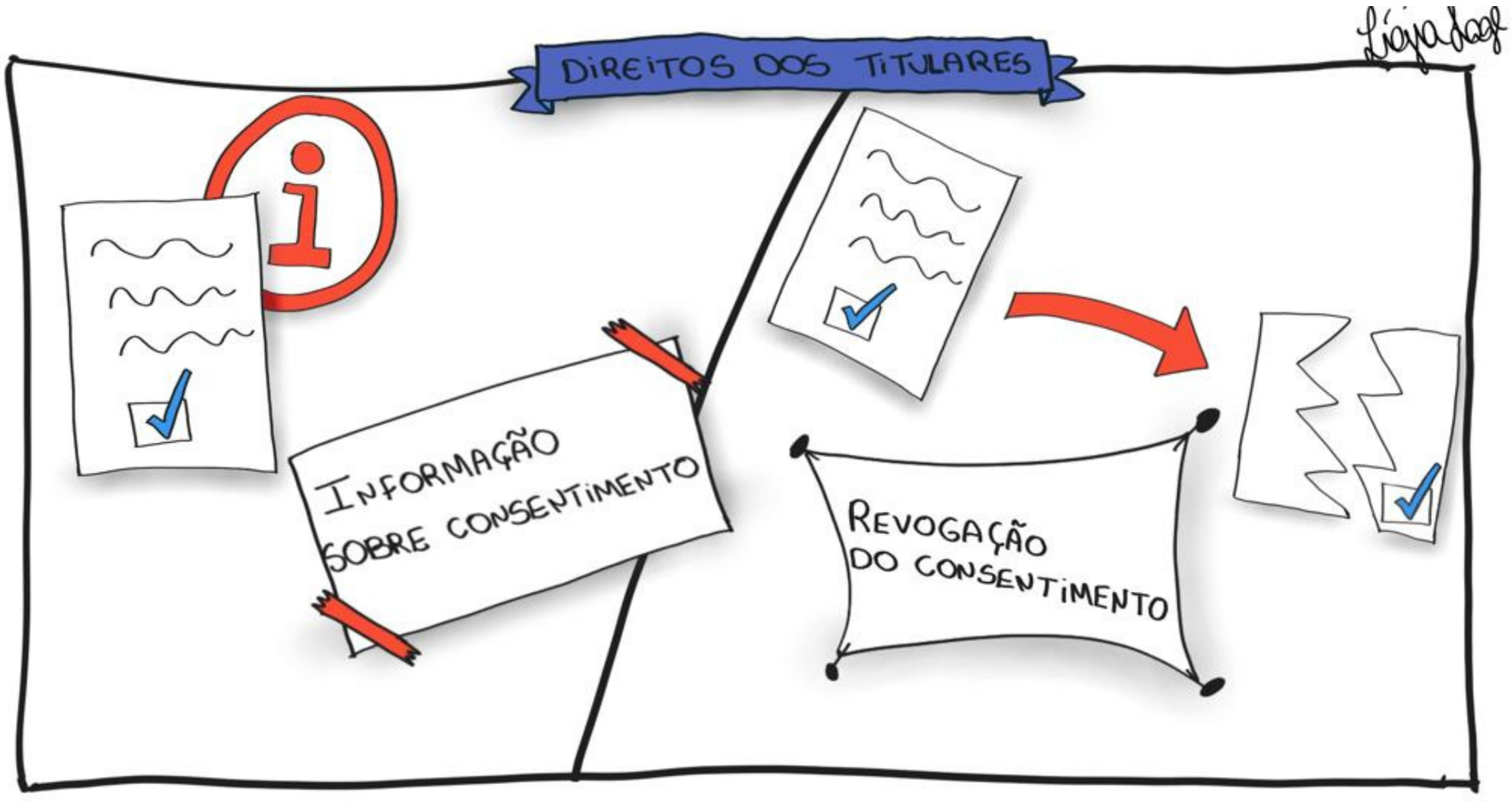
4.Bloqueio ou eliminação de dados pessoais: direito de requerer a suspensão de operações dos dados pessoais pelo consultório ou a sua exclusão quando forem desnecessários, excessivos ou tratados em desconformidade com a LGPD. Você deverá comunicar de forma imediata a todos os operadores para que realizem o mesmo procedimento de forma idêntica.

5.Informação de compartilhamento de dados pessoais: direito de obter do controlador informação das entidades públicas e privadas com as quais foram realizados o compartilhamento de dados pessoais.



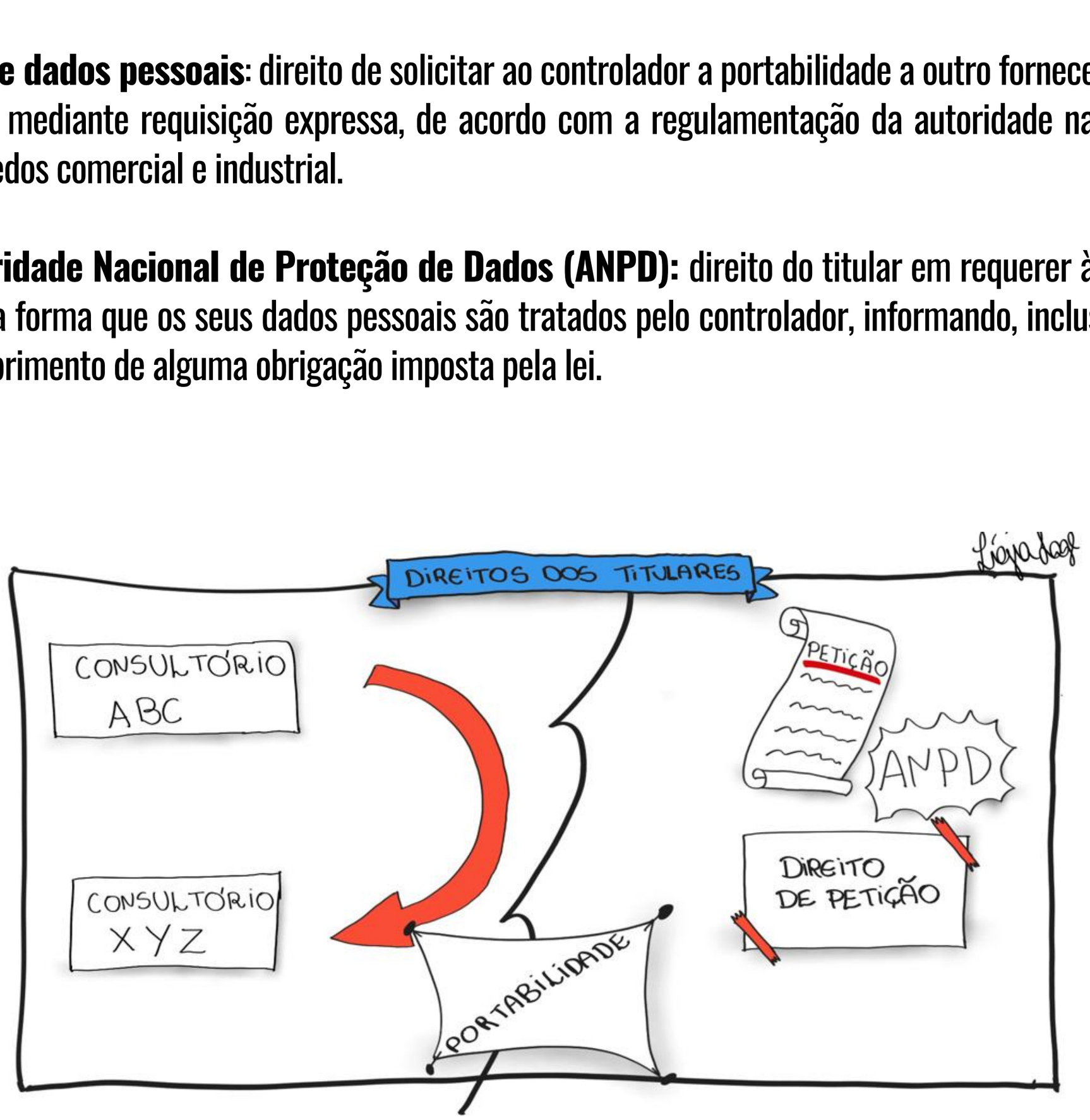
6.Informações sobre a possibilidade de não fornecer o consentimento: direito de obter a informação sobre a possibilidade e as consequências de não fornecer o seu consentimento sobre o tratamento de dados pessoais.

7.Revogação do consentimento: direito do titular de revogar a sua autorização (consentimento) anteriormente concedida para o tratamento dos dados. Você não poderá mais tratar os dados pessoais obtidos com base no consentimento, exceto para finalidades que se encaixem em outra base legal, como por exemplo, cumprimento de obrigação legal e exercício regular de direito.



8.Portabilidade de dados pessoais: direito de solicitar ao controlador a portabilidade a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.

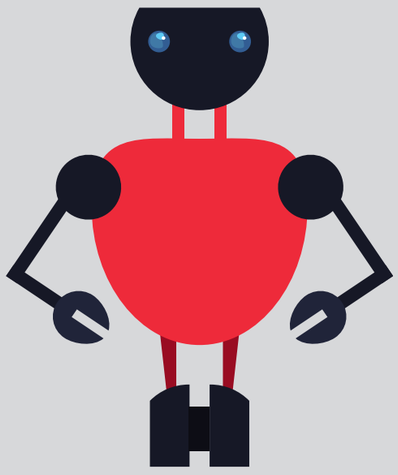
9.Petição à Autoridade Nacional de Proteção de Dados (ANPD): direito do titular em requerer à ANPD a sua avaliação pela forma que os seus dados pessoais são tratados pelo controlador, informando, inclusive de imediato o descumprimento de alguma obrigação imposta pela lei.



10.Não discriminação: direito de não ser tratado de forma discriminatória, ilícita ou abusiva com base nos dados pessoais informados.

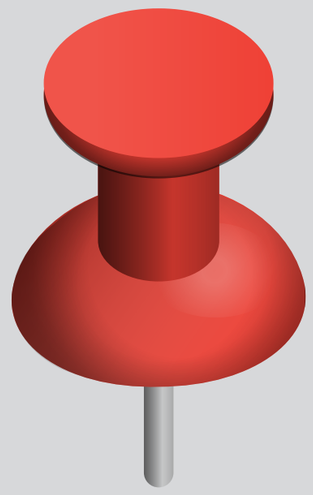
11.Revisão de decisões automatizadas: direito do titular de solicitar a revisão de decisões tomadas exclusivamente com base em tratamento automatizado, incluindo definições de perfis de crédito, consumo, pessoal ou profissional.

12.Oposição ao tratamento: direito de se opor ao tratamento dos seus dados pessoais, quando realizados em desconformidade com os dispostos na LGPD.



ATENÇÃO: Os dados pessoais deverão ser armazenados no formato que favoreça o exercício do direito e a critério do titular, podendo ser fornecidos em formato impresso ou eletrônico. Informações simples devem ser apresentadas imediatamente ao titular e informações mais completas (direito de informação e direito de acesso) dentro do prazo de 15 (quinze) dias a partir da solicitação realizada pelo titular.

O QUE É UM AVISO DE PRIVACIDADE E POLÍTICA DE COOKIES?



Aviso de privacidade é uma maneira clara, acessível e precisa de informar ao titular sobre o tratamento de seus dados.
Ele deve conter as seguintes informações:

- Quais são os dados coletados (ex: nome, endereço, CPF, dados do prontuário);
- Como são protegidos (ex.: sistemas de segurança da informação utilizados);
- Com quem são compartilhados (ex.: operadora de plano de saúde);
- Quais os direitos dos titulares (ex.: acesso aos dados, correção de dados incorretos ou desatualizados (vide tópico de direitos dos titulares);
- Tempo de retenção dos dados (ex. prontuário médico, prazo de 20 anos).

ATENÇÃO: o aviso de privacidade deve estar disponível ao titular no site de seu consultório e em versão impressa na sede de modo a assegurar que todos os pacientes tenham acesso ao seu conteúdo.

E O QUE SÃO COOKIES?

Pequenos arquivos de TEXTO atrelados aos sites, conhecidos por sua capacidade de captura automatizada conforme sua função. Funciona como um tipo de etiqueta exclusiva do site visitado.

E se você tem site, é preciso ficar atento à utilização dos cookies.[1] É imprescindível informar no aviso de cookies os dados pessoais coletados, assim como sua finalidade, devendo ser obervado consentimento específico para cada um deles. Eles estão divididos pelo tipo de dados que capturam e funções que exercem:

Cookies estritamente necessários	Essenciais para o funcionamento do site (exemplo: ferramentas para autenticação do usuário).
Cookies de performance	Melhoram a performance de acordo com o acesso do usuário (exemplo: identificar eventuais erros durante a navegação).
Cookies de funcionalidades	Relacionados a preferências do usuário (exemplo: idioma e região).
Cookies de comportamento (ou de propaganda)	Coletam dados do usuário para criação de perfil de consumo, permitindo a veiculação de publicidade específica e de acordo com as preferências do usuário.
Flash cookies	Permitem a visualização de vídeos, jogos online e sites interativos.
Web beacons	Possibilitam rastrear movimentos feitos pelo usuário no ambiente virtual, (exemplo: identificar se determinada pessoa abriu um e-mail) gravar áudio do computador, compartilhar imagens com terceiros, etc.
Fingerprinting	Viabiliza o direcionamento de publicidade específica para o usuário de acordo com os detalhes do navegador e dos dispositivos utilizados, mas sem o armazenamento de cookies.

[1] Definição dos tipos de cookies e exemplos extraídos do artigo “Cookies - contornos atuais” de autoria de Felipe Palhares, contido na obra “Temas atuais de proteção de dados” - São Paulo: Thomson Reuters Brasil, 2020 - Coordenação Felipe Palhares.

ASPECTOS GERAIS DO PROGRAMA DE PROTEÇÃO DE DADOS

Não há uma regra ou modelo específico para desenhar o programa de adequação à lei, pois ele dependerá, por exemplo, do volume de dados que o consultório trata, a quantidade de colaboradores e fornecedores, os recursos humanos e financeiros disponíveis para implementação, a definição de prioridades e integração com eventuais práticas já existentes.
No entanto, há etapas básicas que devem ser consideradas:

1.CRIAÇÃO DE ESTRUTURA MÍNIMA DE GOVERNANÇA

Exemplo 1- Consultório com apenas uma ou duas pessoas: recomenda-se a contratação de uma consultoria com foco em implementação de programa de proteção de dados que além de ser a responsável pela adequação, terá um de seus integrantes nomeado como DPO do consultório. Salvo futura dispensa pela ANPD.[2]

Exemplo 2 - Consultório que possua áreas específicas, tais como, financeiro, marketing, TI ou jurídico, ou tenha mais sócios, ou ainda, que compartilhe o local com outros profissionais e utilizem os mesmos funcionários, fluxos de dados e sistemas, sugere-se:

- Criação de comitê executivo de proteção de dados que contenha representantes de cada uma das áreas para atuar em conjunto com o encarregado de dados (DPO) nomeado e a consultoria contratada para implementação do programa;
- Criação de grupos de trabalhos, de preferência, que envolvam o jurídico, compliance e segurança da informação.

ATENÇÃO: Ainda que o consultório seja de pequeno ou médio porte é preciso nomear o encarregado de dados (DPO), sendo que a ANPD poderá vir a dispensar essa exigência.

[2]DPO: Art. 5º, VIII, LGPD: Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)

2.CONSCIENTIZAÇÃO

É necessário o comprometimento da alta gestão do consultório, ainda que tenha apenas um sócio, o próprio profissional liberal e uma secretária.
Além de criar diretrizes mínimas para auxiliar na conscientização interna (colaboradores) e externa (fornecedores e pacientes).

Formas de conscientização:

- Treinamentos;
- Workshops;
- Aulas online.

Exemplo 1 - Secretária é responsável pelo agendamento da consulta do paciente, coleta dos dados de eventual plano de saúde, envio de guias para operadoras de planos de saúde, armazenamento dos dados dos pacientes e prontuários, além do envio de dados para contabilidade.

Nesta hipótese, a secretária cumula funções de diferentes áreas, seja de secretariado, seja de financeiro. Assim, ela deverá receber treinamento específico referente a cada tipo de dado que ela trabalha.

ATENÇÃO: os treinamentos devem ser registrados, sejam eles em workshops ou aulas online para fins de demonstração de que o consultório está em processo de implementação do programa de proteção de dados e, posteriormente, sobre a sua manutenção. Aliás, é imprescindível registrar toda a atividade de tratamento.

3.MAPEAMENTO

Esta etapa consiste na realização de um inventário dos dados existentes no consultório para conhecer os fluxos dos dados, identificar gaps, riscos, impactos e desafios.

Pontos importantes do mapeamento:

- Forma como são tratados;
- Classificação;
- Categorização;
- Tempo de retenção;
- Harmonização com legislações setoriais (ex.: ANS).

Uma vez realizado o mapeamento, o relatório de impacto deverá conter as recomendações para sanar os gaps e servirá como referência para os planos de ações a serem traçados a partir deles e executados nas próximas fases do programa.

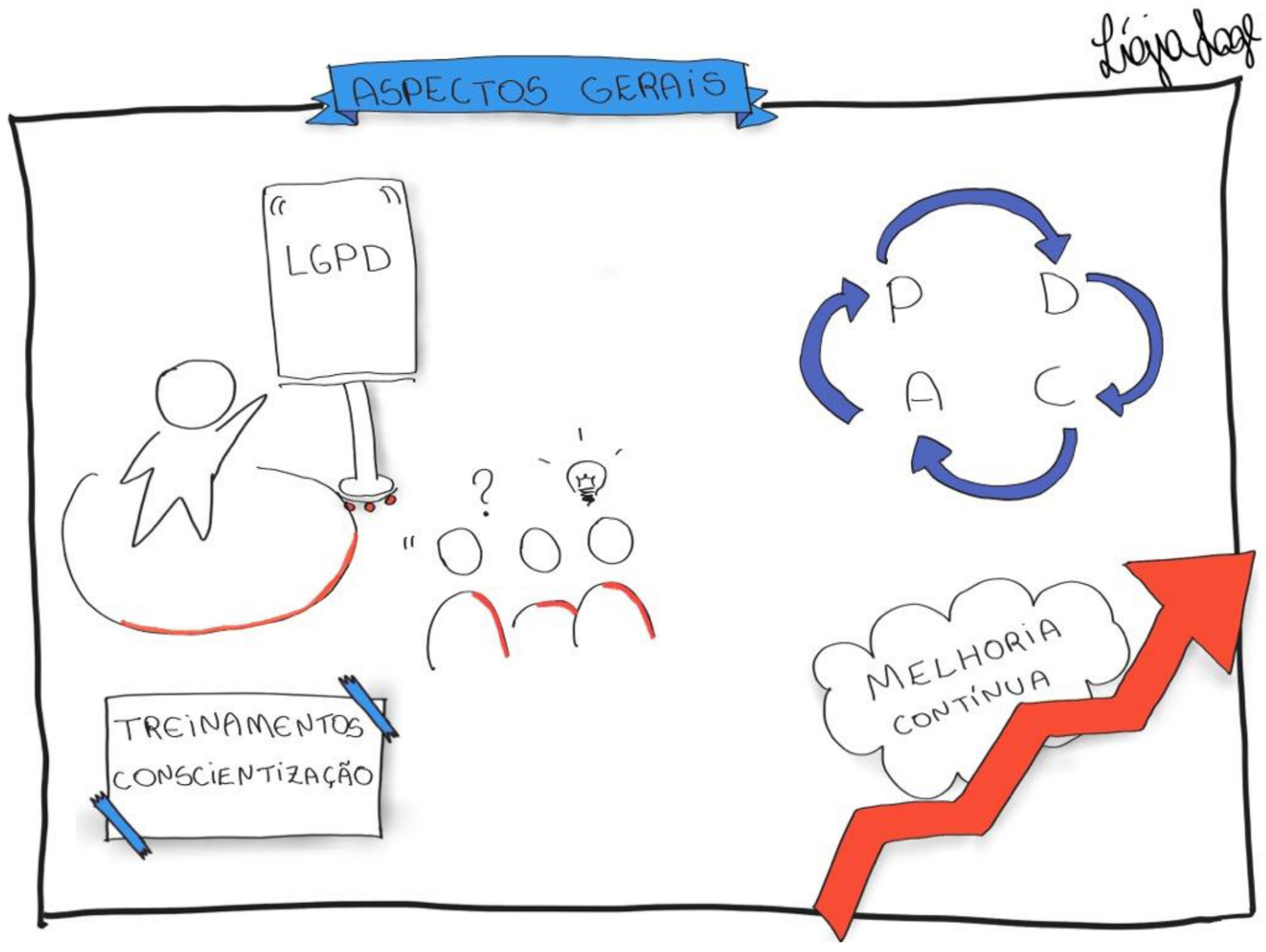
Exemplo 1 - Pergunta do questionário de mapeamento:
Você compartilha o prontuário do paciente via whatsapp?

Se a resposta for NÃO, mas na prática SIM e ocorre este tipo de compartilhamento, isso comprometerá o diagnóstico a ser realizado.
Assim, é importante que os colaboradores respondam com transparência às entrevistas e questionários.

4. IMPLEMENTAÇÃO DE PROGRAMA DE GOVERNANÇA DE DADOS

A implementação de um programa de governança de dados envolve diversas medidas técnicas e organizacionais a serem efetuadas, dentre elas:

- Criação da Política de Dados;
- Composição da estrutura organizacional de governança dos dados com a definição dos nomes e papéis a serem desenvolvidos;
- Responsáveis pelas tomadas de decisão;
- Procedimentos para tomada de decisão;
- Registro de todas as atividades de tratamento dos dados;
- Base legal para o tratamento de dados de acordo com sua classificação e categoria;
- Plano de ação e procedimentos para respostas a incidentes de segurança da informação;
- Plano de ação e procedimentos para respostas de requerimentos dos titulares;
- Elaboração e revisão de documentos: contratos de trabalho, contratos de fornecedores, contratos estratégicos, termo de confidencialidade, aviso de privacidade, aviso de cookies;
- Metodologia de treinamentos;
- Medidas técnicas e administrativas relacionadas à segurança da informação.



5.MONITORAMENTO CONTÍNUO

O projeto de adequação após implementado torna-se um programa de governança, uma vez que os processos e procedimentos são intermináveis e vivem em um verdadeiro ciclo, como um PDCA, por exemplo.

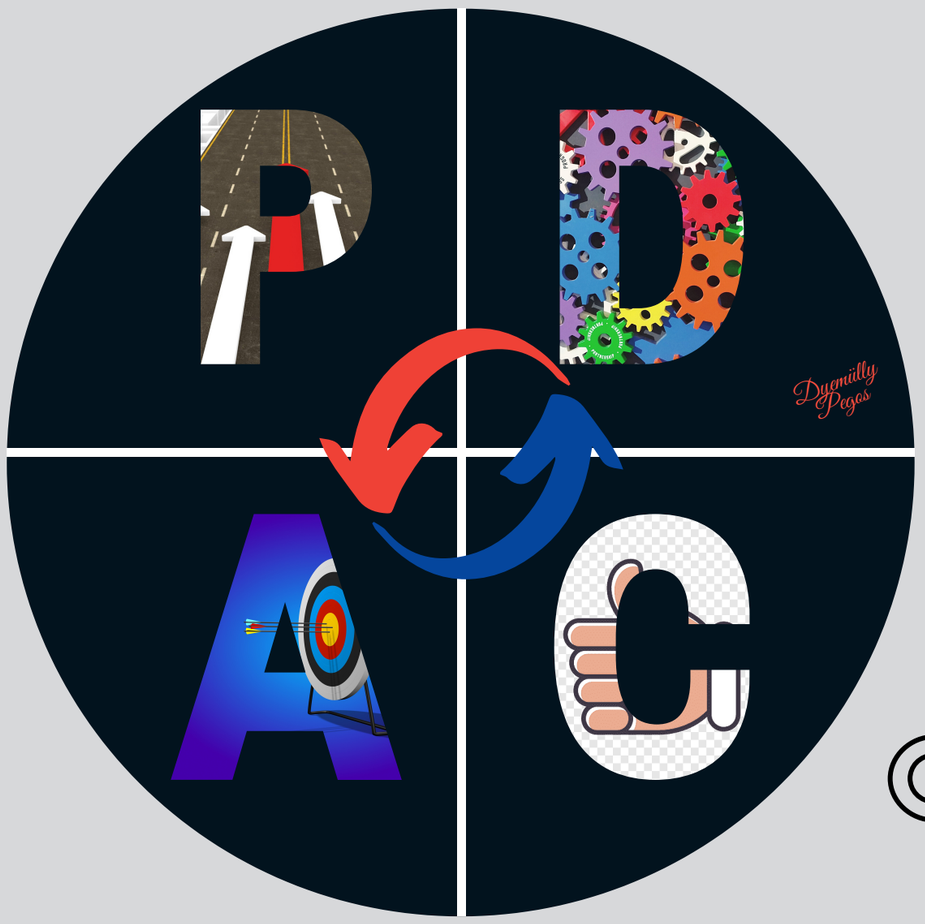
CICLO PDCA

Plan
PLANEJAR

IDENTIFICAR OS PROBLEMAS E PLANEJAR AS MEDIDAS PARA AGIR

Do
FAZER

SEGUIR EXATAMENTE O QUE FOI PLANEJADO "MÃO NA MASSA"



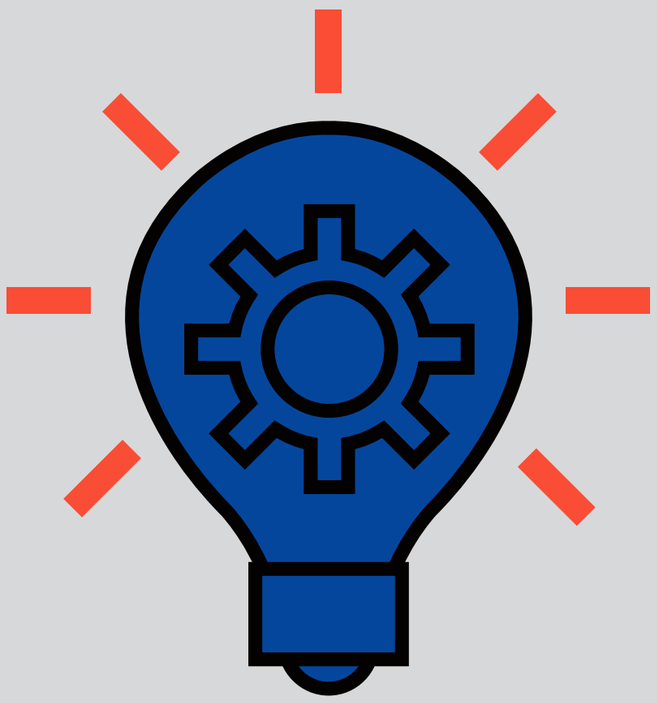
Action
AGIR

VER O QUE NÃO DEU CERTO E IMPLEMENTAR MELHORIAS

Check
CHECAR

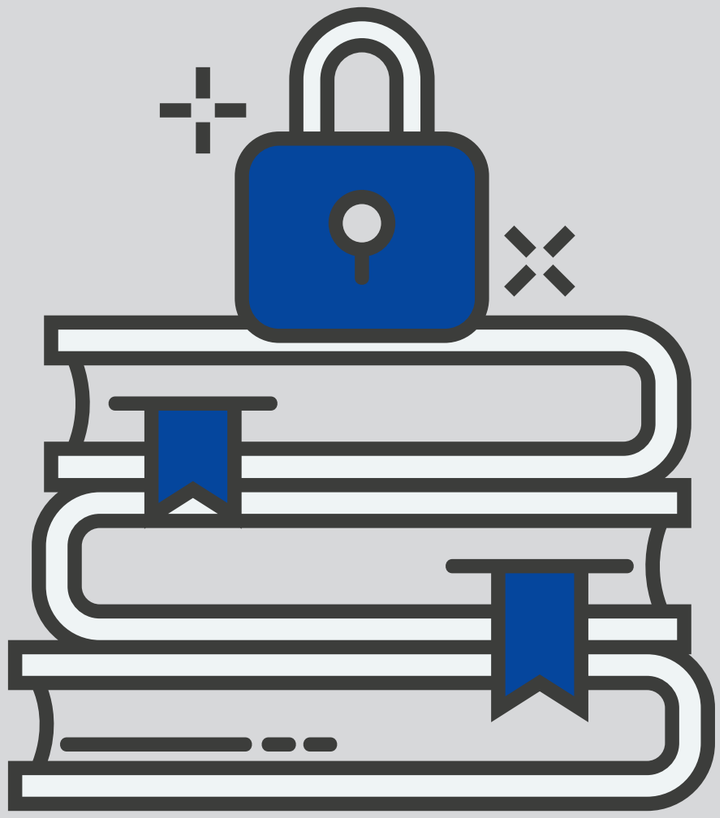
VER SE O OQUE FOI PLANEJADO ESTÁ SENDO SEGUIDO

A definição dos indicadores de sucesso do programa permitirão avaliar as métricas e performance.
Avaliar também se as práticas adotadas estão funcionando, se houve retorno do investimento na implementação do projeto, o valor gerado pelo programa, identificação de eventuais falhas, necessidades de revisões para que se possa ter uma melhoria contínua do processo.



QUAIS MEDIDAS ADMINISTRATIVAS DEVO UTILIZAR PARA TRATAR OS DADOS DOS MEUS PACIENTES?

As medidas técnicas e administrativas são os procedimentos internos que o consultório deve estabelecer durante a implementação do programa de governança com a finalidade de prevenir danos em razão do tratamento de dados.

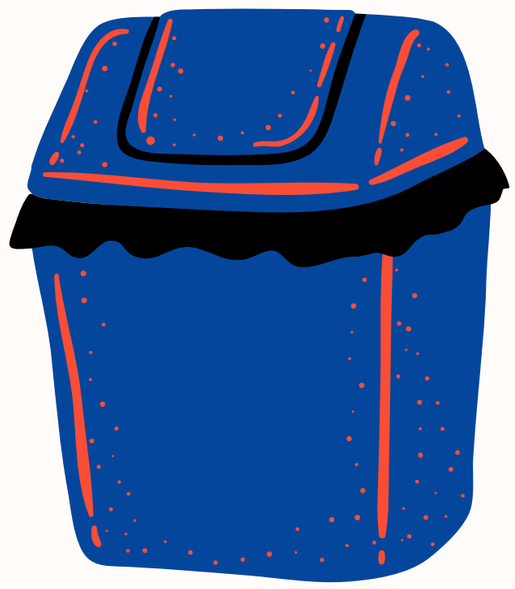


Exemplos:

- Não compartilhar prontuário via whatsapp;
- Armazenar o prontuário em local seguro;
- Restringir o acesso de colaboradores aos dados sensíveis dos pacientes;
- Não deixar documentos e prontuários dos pacientes em impressoras, pois terceiros não autorizados podem ter acesso e isso configurará incidente;
- Triturar documentos com dados pessoais dos pacientes que não são mais necessários e nem possuem finalidade.

ATENÇÃO: o consultório não deverá eliminar documentos que contenham dados pessoais dos pacientes decorrentes do cumprimento de obrigação legal.

Exemplo: o prazo de armazenamento de prontuário médico é de 20 anos a partir do último registro (art. 6º da Lei n.13.787/2018), após é possível a sua eliminação ou devolução ao paciente (art. 6º, §2º).

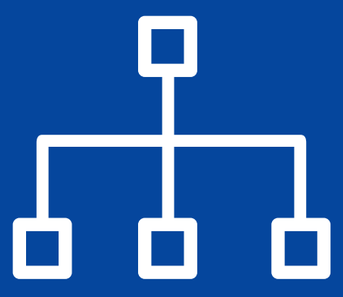


Além do cumprimento de todas as normas exigidas exclusivamente pelos órgãos reguladores do setor da saúde, algumas boas medidas técnicas de segurança da informação são essenciais para o cumprimento da lei.

MEDIDAS TÉCNICAS DE SEGURANÇA DA INFORMAÇÃO

EXECUTAR CÓPIAS DE SEGURANÇA - BACKUP

Ao realizar uma cópia de segurança dos dados processados em um sistema, isso irá prevenir que as informações armazenadas sejam alteradas ou removidas do servidor. Em caso de vírus, ataques cibernéticos ou mesmo por uma imprudência técnica, o backup poderá restaurar a normalidade do sistema e minimizar uma perda enorme de dados tratados. O ideal é sempre manter uma rotina de cópias, que seu armazenamento esteja distante fisicamente dos servidores e que haja um controle de acesso.



CONTROLE DE ACESSO AO SISTEMA POR HIERARQUIA

Esse tipo de medida visa proteger os dados pessoais dos usuários, de modo que os funcionários só tenham acesso aos necessários de suas funções.

Exemplo: Um atendente de faturamento ter acesso ao prontuário do paciente, não faz sentido, então porque disponibilizar acesso?!

A função de habilitar acesso por hierarquia está disponível na maioria dos sistemas, caso negativo, verifique com urgência junto a sua equipe de tecnologia ou fornecedor.

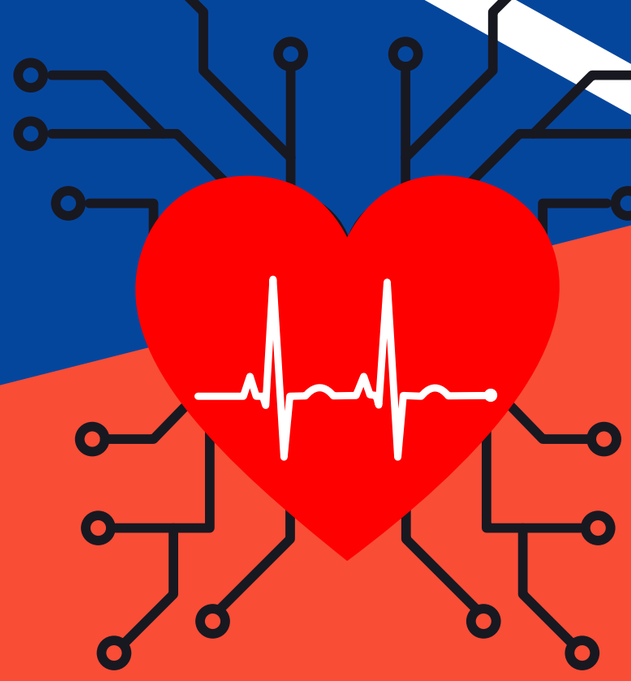
CONTROLE DE ACESSO POR SENHAS

Alguns equipamentos de tecnologia sugerem habilitar senhas, outros por padrão já estão habilitados para trabalhar com este recurso de segurança. Por mais que haja um trabalho de conscientização, o usuário sempre tenta encontrar senhas que possam apresentar uma fixação na memória com menos esforço, muitas vezes tornando-a pública ou de fácil acesso. É importante que esta medida de segurança não seja burlada, implantando, por exemplo, um tempo de vida útil curto, exigindo tamanho mínimo com caracteres especiais, entre outros.

ATUALIZAÇÃO DE SISTEMAS

Com o avanço das tecnologias, todos os programas necessitam de manutenção, melhorias e/ou correções. Por este motivo, de tempos em tempos, são disponibilizadas atualizações por parte do fabricante, que notifica o usuário, por algum canal. É de extrema importância que seja realizada a sua atualização, evitando assim que possíveis defeitos no sistema possam ser utilizados por programas invasores que aproveitam desta deficiência para provocar alguma perda ou dano em seu funcionamento.

Estas poucas medidas relacionadas acima irão dar uma noção da importância das medidas técnicas.

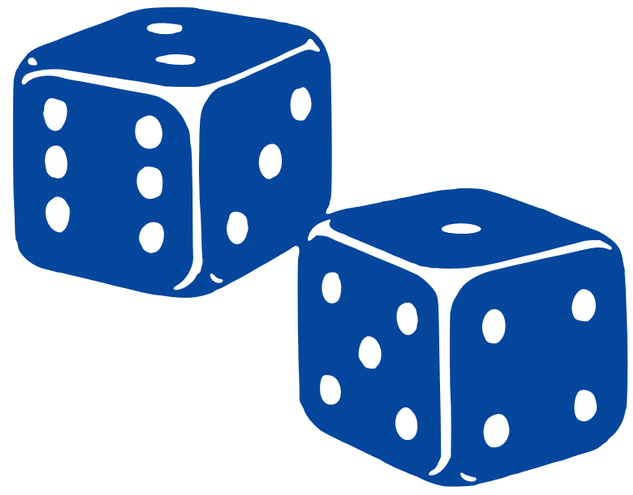


É importante que seja definido ou implantado uma Política de Proteção da Segurança da Informação nos consultórios com as normas necessárias para colaboradores administrativos/técnicos e profissionais da saúde, onde estarão previstas e analisadas todas as medidas técnicas necessárias para o consultório, pois a capacidade de investimento, maturidade da empresa e medidas implantadas irão variar em cada ambiente de tecnologia que tem como propósito a proteção dos dados pessoais.

Essa política deve ser desenvolvida por profissionais qualificados em sua área de atuação e com profundo conhecimento no tratamento dos dados pessoais de acordo com a Lei Geral de Proteção de Dados e demais legislações, notas técnicas entre outros.

Além de cuidar da saúde dos pacientes, é necessário observar o tratamento dos dados pessoais deles, pois isso interfere diretamente em suas vidas.

CONSIDERAÇÕES FINAIS

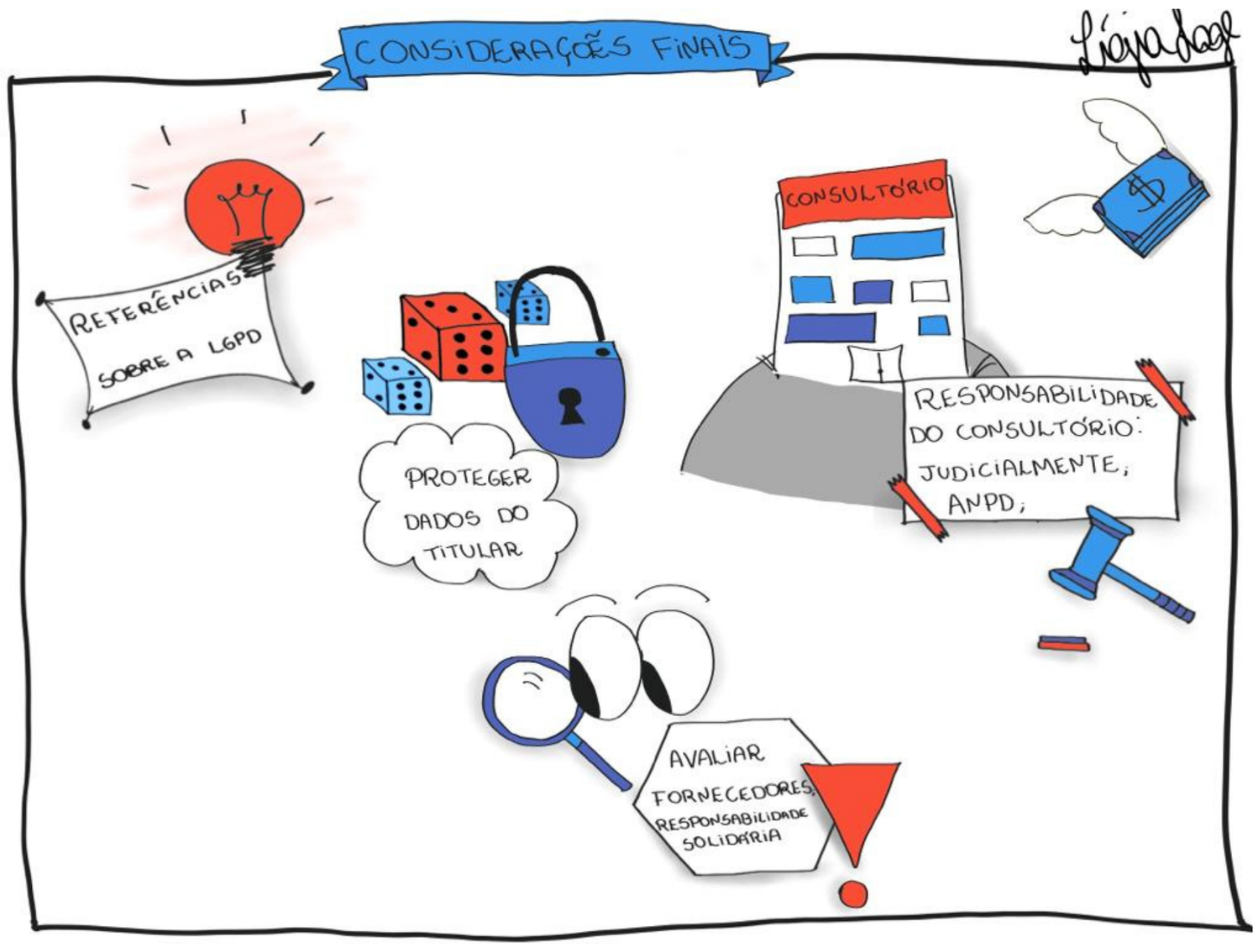


Este material tem por objetivo proporcionar aos profissionais da saúde à aquisição de referências básicas sobre a implementação de um programa de governança de dados em seus estabelecimentos, porém trata-se somente de noções gerais sobre o tema.

É de suma importância a adequação dos profissionais autônomos de saúde, consultórios e clínicas à LGPD, pois nesse segmento são tratados dados pessoais sensíveis. A lei, ainda visa proteger, a liberdade, privacidade e direitos da personalidade do titular, como ser humano.

O consultório/clínica/profissional autônomo da saúde é responsável pelo tratamento dos dados que realiza e pode responder civilmente no âmbito judicial ou administrativamente perante a Autoridade Nacional de Proteção de Dados por eventual descumprimento.

Além disso, é indispensável que os profissionais da saúde avaliem se os seus fornecedores estão em conformidade com a lei, uma vez que a responsabilidade entre o controlador e o operador é solidária e os danos à reputação da empresa decorrentes de um incidente de dados pode ser muito mais maléfico que eventual multa aplicada.



LAB nextlaw academy