PARA CONSULTÓRIOS
ÁREA DA SAÚDE

SÃO PAULO

NOVEMBRO 2021
OABSP

Comissão Especial de Privacidade e Proteção de Dados Pessoais
GT Privacidade na Saúde

Sumário

1 | Palavra da Coordenadoria

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural

Todas as áreas de uma empresa e integrantes de um consultório que tratam dados pessoas no exercício de suas atividades profissionais devem atentar para a privacidade e proteção dos dados pessoais, em conformidade com a LGPD. Na área da Saúde a LGPD apresenta maior nível de exigência e rigor, em razão do volume de dados pessoais sensíveis processadas diariamente

Esta Cartilha foi desenvolvida pelos membros da Coordenação do eixo da Saúde da Comissão de Privacidade e Proteção de Dados da OAB/SP e possui caráter informativo, pois consolida um conjunto de informações que objetivam facilitar a compreensão da Lei Geral de Proteção de Dados (LGPD) e seus impactos, orientando os controladores, encarregados e operadores sobre seus respectivos deveres e destacando os direitos dos titulares de dados pessoais

De forma objetiva e simplificada, a Cartilha apresenta as principais informações sobre a nova Lei Geral de Proteção de Dados para que todos da área da saúde possam avaliar os riscos futuros de sua forma de atuação e planejar mudanças e adequação

Destacamos que o sucesso deste projeto só foi possível graças ao apoio, colaboração e a confiança da Dra. Patricia Peck que, com o seu constante apoio e incentivo ao longo do desenvolvimento desta cartilha, vibrou junto com a Coordenadoria pelos projetos apresentados, sem hesitar em atender às suas demandas. Deste modo e com pura Justiça, a ela dirigimos o nosso sentimento de gratidão!

Agradecemos também a Dra. Rosalia Ometto, por organizar e finalizar todo o material encaminhado pelos membros da Comissão

Por fim, parabenizamos e agradecemos todo empenho, eficiência e dedicação dos membros dessa Coordenadoria

Maria Cristina Gonçalves
Coordenadora do GT de Saúde e Privacidade

2 | Introdução

O setor de saúde já dispõe de uma série de regulações e normas setoriais próprias tais como da Agência Nacional de Saúde Suplementar (ANS), do Conselho Federal de Medicina (CFM), da Agência Nacional de Vigilância Sanitária (Anvisa), do Conselho Nacional de Saúde (CNS), entre outras, envolvendo o sigilo e confidencialidade das informações dos pacientes e usuários do sistema de saúde e daqui em diante deverá se atentar para a privacidade e proteção de dados pessoais dos titulares, conforme regramento trazido pela Lei Geral de Proteção de Dados Pessoais

Nesse sentido, as clínicas e os consultórios da área de saúde deverão adotar medidas que garantam o tratamento de dados pessoais de forma adequada, respeitando os princípios trazidos pela LGPD, em especial, os da finalidade, necessidade e transparência, de forma que sejam usados somente os dados pessoais imprescindíveis com fins específicos e informados ao titular, sempre em respeito à sua privacidade e de acordo com as bases legais autorizadoras do tratamento. Grande parte dos dados pessoais tratados no setor da saúde diz respeito a dados pessoais sensíveis, mas há ainda os dados pessoais dos funcionários, fornecedores e prestadores de serviços

De maneira adicional, as clínicas e os consultórios deverão reforçar os cuidados relacionados à manutenção da confidencialidade dos documentos do paciente, principalmente seu prontuário médico, garantindo que eles sejam armazenados de forma segura física, como digital e acessados somente pelos profissionais que de fato necessitem ter conhecimento das informações clínicas do paciente. As clínicas e consultórios devem manter um sistema de segurança adequado para evitar incidentes

A confidencialidade e a proteção de dados pessoais sempre estiveram presentes no setor de saúde, portanto, a aplicação da LGPD às operações de tratamento de dados nesse setor consagra e consolida essas figuras jurídicas de forma expressa. Os mecanismos previstos na LGPD são capazes de garantir o emprego sustentável e útil de dados pessoais e dados pessoais sensíveis, assegurando ao mesmo tempo aos titulares o exercício de seus direitos

DADOS PESSOAIS
COMBINAM COM
Finalidade
Necessidade
Transparência

PROFISSIONAIS DA SAÚDE
Dados de saúde são
dados pessoais sensíveis
precisam de mais cuidado

PALAVRAS-CHAVE
Confidencialidade
Sigilo

1

3 | Conceitos para aplicação prática em clínicas e consultórios da área da saúde

3.1 | Como a LGPD se aplica às clínicas e os consultórios da àrea da saúde?

A Lei Geral de Proteção de Dados (LGPD), conforme estabelece seu art. 1°, se aplica à pessoa natural ou pessoa jurídica de direito público ou privado que realize tratamento de dados pessoais, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

(i) a operação de tratamento seja realizada no território nacional;

(ii) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou

(iii) os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

3.2 | Qual objetivo da LGPD?

Importante frisar que o Brasil não é pioneiro na criação de normas de proteção de dados

Em verdade, o Brasil seguiu a tendência mundial ao publicar a Lei n. 13.709 em 14 de agosto de 2018, que entrou em vigor 18/09/2020, com aplicação de penalidades administrativas a partir de 01/08/2021.

As normas de proteção de dados espalhadas pelo mundo refletem a preocupação em preservar o uso adequado dos dados pessoais, garantindo, desta forma, a preservação de direitos fundamentais, como o da privacidade, da liberdade e do livre desenvolvimento da personalidade da pessoa natural

QUER CONHECER TEXTOS DE LEI?
Procure sempre
Sites oficiais
Portal da Legislação

QUER CONHECER O TEXTO DA LEI 13.709/18 – LGPD?
Acesse aqui

2

3 | Conceitos para aplicação prática em clínicas e consultórios da área da saúde

3.3 | O que são dados

PESSOAIS

Dado pessoal é uma informação relacionada a pessoa natural identificada ou identificável (art. 5°., inciso I da LGPD)

- Tudo que identifica uma pessoa humana viva
- De forma direta
  ou
- Somadas chegam a uma pessoa humana específica ou determinada

3

Exemplos:

Identificação DIRETA
Nome, CPF, RG, CNH, CFM, CRO, CREFIPO, COREN etc.

Identificação que PODE CHEGAR a uma pessoa específica
Endereço, e-mail, IP (número do computador), tatuagens, geolocalização, data de nascimento etc.

PESSOAIS SENSÍVEIS

Por outro lado, o dado pessoal sensível é o que diz respeito à origem racial ou étnica, 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 (art. 5°, inciso II da LGPD)

- São dados pessoais que podem gerar preconceitos ou discriminações, bem como, muito importantes como a biometria (normalmente recolhendo digitais das pessoas) e genéticos (cada pessoa humana é única e diferente em seu conteúdo genético)

4

Exemplos área da saúde:

Informações sobre doenças, riscos de doenças, relatórios médicos, prontuários, resultados de exames, moldes odontológicos, dados biométricos, informações genéticas etc.

3 | Conceitos para aplicação prática em clínicas e consultórios da área da saúde

3.4 | O que são dados pessoais?

De acordo com a LGPD qualquer operação realizada com um dado pessoal é chamada de tratamento de dados, como as que se referem a coleta, produção, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (art. 5°., inciso X da LGPD)

Todo tipo de estabelecimento de saúde trata dados pessoais, em maior ou menor quantidade, e as obrigações da LGPD se somarão às obrigações específicas da área, tais como vigilância sanitária, dos conselhos de especialidade, da ANS, do SUS, entre outras.

5

3.4.1 | Algumas hipóteses de tratamento de dados pessoais em estabelecimentos de saúde

- Cadastro de paciente
- Elaboração de prontuário médico, odontológico, nutricional etc.
- Armazenamento de prontuários de saúde, em papel ou em formato digital
- Compartilhamento de informação sobre plano de saúde, odontológicos
- Destruição de prontuários de saúde antigos
- Transmissão, de um estabelecimento de saúde para outro, de informações sobre o estado de saúde de paciente (titular dos dados pessoais)
- Coleta, por farmácias, da prescrição médica, odontológica, nutricional, de consumidor (titular dos dados pessoais) para fornecimento de medicamentos e posterior arquivamento

3 | Conceitos para aplicação prática em clínicas e consultórios da área da saúde

3.5 | Quem são as partes envolvidas no tratamento de dados pessoais?

TITULAR

Titular é pessoa natural (pessoa física, viva) a quem se referem os dados pessoais que são objetos de tratamento)

Exemplos de titulares de dados pessoais em clínicas, consultórios, hospitais:

Pessoas que são atendidas; visitantes com dado pessoal colhido na recepção; prestadores de serviço; funcionário do consultório e ainda todos os sócios, pessoas naturais

CONTROLADOR

Controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.

Possibilidade de tratamento de dados pessoais em decorrência de legislação ou norma específica que assim o exija.

Quem tem o contato direto e primeiro com o titular de dados pessoais

Exemplos de controladores:

As próprias clínicas e consultórios de qualquer área da saúde serão responsáveis, podem figurar como controladores, se os dados pessoais lhes forem entregues direta e primeiramente

- Quando a clínica faz coleta dos dados na recepção para cadastro e quando paciente passa com profissional da área de saúde, que irá coletar mais dados para inserir no prontuário

OPERADOR

Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador

Recebe os dados pessoais via controlador

Exemplos de operadores:

Empresa contratada para instalação de câmeras de segurança. O controlador é quem indica onde serão instaladas as câmeras, quem poderá acessar as imagens e qual o prazo de armazenamento. A gravação e armazenamento são efetuados pela empresa contratada, que será operadora nesse caso, pois realiza tratamento dos dados pessoais em nome do controlador

Contador que recebe informações para realizar a contabilidade geral, departamento pessoal

ENCARREGADO

Encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre: o controlador, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD)

ANPD

Autoridade Nacional de Proteção de Dados (ANPD) é a autoridade tem entre outras atribuições dispostas na legislação: editar regulamentos, ouvir a sociedade em matérias de interesse relevante, deliberar sobre a aplicação da lei, fiscalizar o cumprimento da LGPD e aplicar sanções, conforme o seu art. 55-J da LGPD

Sobre Controladoria Conjunta

Cabe destacar ainda, que uma mesma operação de tratamento de dados pessoais, poderá envolver uma controladoria conjunta, o que se extrai do artigo 42, §1°, II, LGPD, quando mais de um controlador estiver diretamente envolvido no tratamento do qual decorram danos ao titular de dados pessoais, estes responderão de forma solidária (conjunta), à exceção das hipóteses previstas no art. 43

Neste sentido a controladoria conjunta implica consequências no que diz respeito às funções dos agentes de tratamento e aos direitos dos titulares, bem como a responsabilidade dos controladores será solidária

O Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado (ANPD) Maio/2021, exemplifica da seguinte forma:

"Uso de dados abertos disponibilizados por Agência Reguladora disponibiliza acesso público aos dados relativos às outorgas dos serviços regulados, incluindo informações de pessoas naturais sócias de prestadoras. A base de dados é armazenada pela própria Agência e utilizada para subsidiar decisões administrativas. Organização da Sociedade Civil tem acesso aos dados disponibilizados pela Agência e efetua, com base em solução de inteligência artificial, cruzamento com outras bases de dados visando à realização de ações de controle social de entidades e agentes públicos. Sociedade Empresária também trata os dados em questão, visando, porém, fornecer serviços de consultoria aos agentes do setor regulado. Embora a mesma base de dados seja utilizada pelas três entidades (Agência Reguladora, Organização da Sociedade Civil e Sociedade Empresária), cada uma dessas organizações é responsável e responde pelos respectivos tratamentos realizados. Neste contexto, não há controladoria conjunta pois o tratamento de dados ocorre no âmbito das atividades e das finalidades definidas por cada organização."

6

Será conferida a controladoria conjunta, se demonstrado todos os requisitos aplicáveis:

1. Mais de um controlador possui poder de decisão sobre o tratamento de dados pessoais

2. Há interesse mútuo de dois ou mais controladores, com base em finalidades próprias, sobre um mesmo tratamento, e

3. Dois ou mais controladores tomam decisões comuns ou convergentes sobre as finalidades e elementos essenciais do tratamento

Dispõe sobre a controladoria conjunta o artigo 26 do GDPR (lei européia de proteção da dados pessoais), ocorre quando há uma "participação conjunta" na determinação de "finalidades e meios de tratamento, mas ão haverá controladoria conjunta se os objetivos do tratamento forem distintos

"Quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento. Estes determinam, por acordo entre si e de modo transparente as respectivas responsabilidades pelo cumprimento do presente regulamento, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados e aos respetivos deveres de fornecer as informações referidas nos artigos 13° e 14°, a menos e na medida em que as suas responsabilidades respectivas sejam determinadas pelo direito da União ou do Estado-Membro a que se estejam sujeitos. O acordo pode designar um ponto de contacto para os titulares dos dados."

3 | Conceitos para aplicação prática em clínicas e consultórios da área da saúde

3.6 | quando os estabelecimentos de saúde podem realizar o tratamento de dados pessoais?

A LGPD trouxe hipóteses em que os dados pessoais e os dados pessoais sensíveis podem ser utilizados, conforme tabelas abaixo:

PESSOAIS (LGPD, art. 7º)

- I - mediante o fornecimento de consentimento pelo titular
- II - sem fornecimento de consentimento do titular, nas hipóteses necessárias para
  - cumprimento de **obrigação legal** ou **regulatória** pelo controlador
  - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de **políticas públicas previstas em leis** e **regulamentos ou respaldadas em contratos, convênios** ou instrumentos congêneres, observadas as disposições do Capítulo IV da LGPD
  - realização de **estudos por órgão de pesquisa,** garantida, sempre que possível, a anonimização dos dados pessoais
  - para a **execução de contrato** ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados pessoais, quando necessário
  - **exercício regular de direitos** em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)
  - **proteção da vida** ou da incolumidade física do titular ou de terceiro
  - **tutela da saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária
  - quando necessário para atender aos **interesses legítimos do controlador** ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, ou
  - **proteção do crédito**, inclusive quanto ao disposto na legislação pertinente

PESSOAIS SENSÍVEIS (LGPD, art. 11)

- I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas
- II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
  - cumprimento de **obrigação legal** ou **regulatória** pelo controlador
  - tratamento compartilhado de dados necessários à execução, pela administração pública, de **políticas públicas previstas em leis ou regulamentos**
  - realização de **estudos por órgão de pesquisa,** garantida, sempre que possível, a anonimização dos dados pessoais sensíveis
  - **exercício regular de direitos**, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)
  - **proteção da vida** ou da incolumidade física do titular ou de terceiro
  - **tutela da saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária
  - **garantia da prevenção à fraude e à segurança do titular**, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais

3 | Conceitos para aplicação prática em clínicas e consultórios da área da saúde

3.6.1 | Principais bases legais para as atividades de clínicas e consultórios da área da saúde

TUTELA DA SAÚDE

aplicada exclusivamente a procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária

EXECUÇÃO DE CONTRATO

possibilidade de tratamento de dados pessoais em virtude de um contrato.

Exemplo: Contrato de trabalho com auxiliar de enfermagem

CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA

possibilidade de tratamento de dados em decorrência de legislação ou norma específica.

Exemplo: Os prontuários médicos que devem ser armazenados por 20 anos após sua última atualização, conforme dispõe a Resolução CFM n. 1.821/2007

CONSENTIMENTO TITULAR

no contexto dos consultórios médicos e de toda área da saúde, o consentimento será uma base de dados secundária, ou seja, apenas deve ser utilizado quando não for possível fundamentar em outra base legal.

O consentimento deve ser uma manifestação livre, informada, inequívoca do titular para o uso de seus dados pessoais para uma determinada finalidade.

Esse consentimento da LGPD se soma ao consentimento ético e de consumidor para tratamentos de saúde

Exemplo: Paciente conseguiu obter o resultado esperado em uma cirurgia e o médico deseja publicar uma imagem em suas redes sociais, neste caso deve-se obter o consentimento do paciente para utilização da imagem

3 | Conceitos para aplicação prática em clínicas e consultórios da área da saúde

É permitido o tratamento de dados pessoais, também, para:

a PROTEÇÃO DA VIDA ou da incolumidade física do titular ou de terceiro

acontece, por exemplo, quando uma pessoa inconsciente dá entrada em um hospital que nunca esteve. Nesse caso, o hospital precisará acessar seus documentos pessoais, dados de convênio médico e de todo o histórico médico desse paciente que um outro hospital haja vista o interesse público envolvido neste tipo de tratamento

É permitido o tratamento de dados pessoais, também, para: a realização de ESTUDOS POR ÓRGÃO DE PESQUISA

essa base legal é apenas para finalidade de pesquisa científicas, tecnológicas, históricas etc., a empresa tem que estar enquadrada em seu contrato social como órgão de pesquisa

Para legitimar o tratamento de dados pessoais com esta base legal para realização de estudos são **necessários ainda alguns cuidados:**

- que a **finalidade** deste tratamento seja a realização de pesquisa científica, histórica, estatística ou tecnológica, por meio de órgão de pesquisa devidamente registrado, ou seja, não é para qualquer pesquisa
- por meio de órgão de pesquisa, também definido no art. 5°, XVIII "órgão de pesquisa é um órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado **sem fins lucrativos** legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico", ou seja, órgão, entidade ou pessoa jurídica cuja **atividade é a pesquisa**
- sempre que possível anonimizando os dados pessoais;
- todos os demais aspectos ligados aos princípios legais serão respeitados

3 | Conceitos para aplicação prática em clínicas e consultórios da área da saúde

3.7 | Tratamento de dados pessoais de crianças e adolescentes

- CRIANÇA – 0 a 12 anos incompletos (ECA)
- ADOLESCENTE – 12 a 18 anos incompletos (ECA)
- MENOR DE IDADE – 0 a 18 anos (CC)
- MENORES ABSOLUTAMENTE INCAPAZES (CC, depende de pais ou responsáveis) – 0 a 16 anos incompletos
- MENORES RELATIVAMENTE INCAPAZES – (CC, tem alguma autonomia, mas os pais e responsáveis ainda respondem civilmente pelos seus atos) 16 a 18 anos incompletos
- MAIORIDADE CIVIL– acima de 18 anos

O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos do artigo 14 da LGPD e também do ECA.

Isso se deve porque a criança e o adolescente deve ter uma proteção especial, pela sua própria falta de compreensão dos fatos e falta de maturidade necessárias para exercer plenamente seus direitos de titular de dados pessoais, em especial com relação a dados pessoais de saúde.

Para crianças, deve ser realizado **sempre** com o **consentimento específico e em destaque** dado por pelo menos um dos pais ou pelo responsável legal.

A questão em discussão entre os doutrinadores, sobretudo, é a questão da análise do consentimento específico de um dos pais ou representante legal em relação ao adolescente. A LGPD não exige, mas o ECA do grau de compreensão e o CC determina a responsabilidade de pais e responsáveis legais até atingir a maioridade civil, pelos atos dos menores.

Quanto mais próximo da maioridade civil, considera-se que o adoslescente tenha mais autonomia para decisão quanto ao consentimento específico e destacado de tratamento de seus de dados pessoais, sem a necessidade representatividade um dos pais ou responsável legal, uma vez que não é obrigatório pela LGPD.

Entretanto, CC, os adolescentes entre 12 e 16 anos, integram o rol dos absolutamente incapazes para os atos da vida civil e serão considerados **nulos**, se realizados sem a representatividade dos pais ou responsáveis legais.

REFERÊNCIAS LEGAIS

LGPD (Lei Geral de Proteção de Dados)
Art. 14, § 1° e 3° consentimento específico e destacado para tratamento de crianças

ECA (Estatuto da Criança e do Adolescente)
Art. 100, IV – interesse superior da criança e do adolescente
Art. 100, XI – obrigatoriedade da informação

CC (Código Civil)
Art. 3° - menores absolutamente incapazes
Art. 4°, I – menores relativamente incapazes
Art. 180 – menor relativamente capaz obriga-se quando se declara dolosamente maior
Art. 932, I e II – responsabilidade objetiva pais e responsáveis legais

3 | Conceitos para aplicação prática em clínicas e consultórios da área da saúde

A lei prevê exceção à regra acima quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção (art. 14, § 3° LGPD)

Em nenhum caso os dados pessoais de criança ou adolescente poderão ser repassados a terceiro sem o consentimento de pelo menos um dos pais ou pelo responsável legal

7

BOA PRÁTICAS | ADOLESCENTES e DADOS DE SAÚDE

- Os dados pessoais sensíveis mais delicados são os relacionados à adolescentes. A regra da LGPD deixou muitas questões em aberto e com alguns pontos de dúvida quando analisado o contexto legal geral. Assim, alguns pontos podem ajudar o profissional nessa decisão no caso específico
- Atender o melhor interesse de saúde da(o) adolescente
- Menores de 16 anos são absolutamente incapazes na vida civil de praticar atos, a melhor conduta, se possível, pegar consentimento específico e destacado de um dos pais ou responsável
- No conflito entre os interesses de saúde da(o) adolescente e adultos, prevalecer os interesses de saúde da(o) adolescente, em especial o relativamente incapaz (entre 16 e 18 anos)
- Pela ética médica e das outras áreas de saúde, o foco da atenção médica é sempre a(o) paciente e sua saúde

3 | Conceitos para aplicação prática em clínicas e consultórios da área da saúde

3.8 | Compartilhamento de dados pessoais tratados

O compartilhamento de dados pessoais pode ocorrer de diversas maneiras, como divulgação de dados, transferência internacional de dados, comunicação a terceiros ou tratamento de dados em bases compartilhadas

Para a regularidade do compartilhamento, é importante observar sempre a finalidade, os princípios da LGPD e as hipóteses de tratamento destes dados

Os titulares devem ter ciência de que seus dados são compartilhados e para quais finalidades específicas, o que pode ser feito através da Política de Privacidade

No âmbito das clínicas e consultórios médicos o compartilhamento pode ocorrer por diversas finalidades

Em determinados casos faz-se necessária à coleta do consentimento ao titular

Exemplo: Consultório faz parceria com um salão de beleza, compartilhando dados pessoais não sensíveis e mínimos necessários de seus pacientes, desde que não tenha participação societária no salão, com o intuito de melhorar a autoestima de paciente, mas apenas para quem desejem receber oferta de combos e participar de sorteios de dia de beleza, bem como informações sobre produtos que lhe possam ser úteis. Necessário coletar o consentimento dessa(e) paciente

Em outras situações, não há necessidade de consentimento, como no caso de prestar informações aos planos de saúde sobre consultas ou procedimentos realizados pelos pacientes conveniados, pois visa atender norma regulamentadora

Exemplos área da saúde:

Compartilhamento de dados pessoais e dados pessoais sensíveis com a ANS e/ou com o SUS para fins de prestação de serviços de saúde e de cobrança, por exemplo

- O titular de dados pessoais tem que estar ciente por onde seus dados pessoais percorrem nos processos da prestação de serviços de saúde
- O foco na informação e transparência ganham relevância, uma camada que se soma às do Código de Defesa do Consumidor (CDC, arts. 6°, III e 31)
- Os Códigos de Ética profissionais estabelecem como regra letra LEGÍVEL para preenchimento dos prontuários

8

4 | Conformidade com a LGPD das clínicas e consultórios

A LGPD impõe aos consultórios e clínicas uma mudança de postura por parte dos seus profissionais, intensificando o aculturamento que privilegie a proteção de dados pessoais, disseminando o conhecimento uniforme de todos os procedimentos estabelecidos para manutenção do programa de privacidade a ser obtido por meio de gestão de boas práticas relativas ao tema

Todos os profissionais, colaboradores e parceiros das clínicas e consultórios, sem exceção, devem estar engajados para cumprimento do programa de proteção de dados pessoais estabelecido, com o objetivo de se evitar quaisquer tratamentos de dados pessoais, especialmente sensíveis, fora do escopo da finalidade e necessidade desses tratamentos, evitando-se riscos aos titulares de dados pessoais, condenações judiciais e sanções administrativas impostas pela autoridade nacional (ANPD) por descumprimento de normas previstas na lei

PROVIDÊNCIAS A SEREM ADOTADAS

1. Nomear Encarregado de proteção de dados, também denominado de DPO (Data Protection Officer)

2. Disponibilizar canal de comunicação para com os titulares

3. Mapear e registrar as operações de tratamento de dados, identificando, minimamente:

   (i) quais dados pessoais tratados em cada operação

   (ii) necessidade de cada dado

   (iii) onde os dados pessoais estão armazenados, seja em uma plataforma específica ou em uma pasta ou planilha

   (iv) quem tem acesso

   (v) bases legais correspondentes

   (vi) compartilhamento com quem

4. Elaborar ou atualizar normas e políticas internas para o tratamento dos dados pessoais, limitando o acesso aos dados pessoais tratados por meio de perfis e senhas

5. Atualizar instrumentos contratuais que envolvam dados pessoais e compartilhamentos

6. Realizar treinamentos e conscientização dos colaboradores e parceiros sobre proteção de dados pessoais, que contemplem questões do espaço físico e acesso restrito ao mínimo de colaboradores possível

7. Elaborar ou atualizar os termos de consentimento

8. Elaborar relatórios de Impacto e proteção de dados pessoais, quando for o caso

9. Analisar sistema de segurança da informação

10. Eliminar documentos com dados pessoais sem previsão legal para tratar

11. Eliminar documentos após o prazo de retenção expirar

12. Dar atenção à segurança do espaço físico do consultório, tais como alarme, travas nas janelas, portas e armários trancados e com acesso restrito ao mínimo possível

4 | Conformidade com a LGPD das clínicas e consultórios

Sugestão de documentos para se buscar a conformidade com a LGPD

DOCUMENTOS PRINCIPAIS	REFERÊNCIAS LGPD
Política de Proteção de Dados Pessoais	Art. 46 - §§ 1° e 2°
Política de Privacidade	Art. 9° - incisos I – II – III ou V
Política de Privacidade para Colaboradores e Alta Gestão	Art. 9°
Política para exercício de direitos pelo titular (incluindo formulário)	Arts. 8° § 5°, 9° § 2°, 17, 18, 19, 20, 21 e 22
Política de Retenção de Dados (Tabela de temporalidade)	Arts. 6° - incisos II – III e IV, 9 – inciso II e 40.
Formulário de Consentimento de titular	Arts. 7° - inciso I, §§ 4° e 5°, 8° §§ 1° ao 6° e 11 – inciso I
Formulário de Consentimento dos pais ou responsáveis	Art. 14 §§ 1° ao 3°
Nomeação do Encarregado (DPO)	Art. 41
Registro (inventário de todas as atividades de processamento)	Art. 37
Notificação de violação de dados pessoais (controlador para ANPD - quando aplicável)	Art. 48
Notificação de violação de dados pessoais (controlador para titular - quando aplicável)	Art. 48
Procedimento de resposta e notificação de violação de dados pessoais	Art. 50 alínea g
Registro de violação de dados pessoais	Arts. 31 e 42

DOCUMENTO ESSENCIAL – a depender da realidade da clínica, consultório, laboratório, hospital etc.	REFERÊNCIAS LGPD
Relatório de Impacto	Arts. 10 § 3° e 38

DOCUMENTOS – BOAS PRÁTICAS	REFERÊNCIAS LGPD
Contrato de processamento de dados pessoais do fornecedor	Artigos 39 e 7° - inciso III
Cláusulas em contratos com operadores e com terceiros, incluindo transferências internacionais, se houver	Artigos 33, 34, 35, 39, 44 e 50
Atas de reuniões de aprovação de políticas e reuniões de comitês de privacidade, de preferência digital e assinaturas eletrônicas	
Registro de treinamento dos colaboradores e da alta gestão, de preferência com certificados de participação	
Treinamento sobre questão de segurança e restrição de acesso aos espaços físicos, com limitação de acesso ao mínimo possível.	
Boas práticas específicas para telemedicina, nos termos das resoluções do Conselho Federal de Medicina	
Adoção de prontuários eletrônicos, com acesso restrito, assinaturas eletrônicas em prontuários e receituários, nos termos das resoluções do Conselho Federal de Medicina	

5 | Dicas para implementação em estabelecimentos de saúde

5.1 | Canal de comunicação com o público, facilitado para tratar da LGPD

Para a implementação (implantação) da LGPD nos estabelecimentos de saúde é de fundamental importância estabelecer um canal de comunicação com os titulares de dados pessoais, que viabilize o exercício dos seus direitos e a garantia da transparência, de forma a facilitar a experiência do usuário, de fácil acesso e compreensão dos procedimentos que o titular deve adotar. Tal canal deve possibilitar que os titulares de dados pessoais solicitem informações sobre a proteção de dados pessoais, sobre as medidas de privacidade adotadas pela sua empresa e sobre o "ciclo de vida" dos dados pessoais por ela tratados

SOU TITULAR DE DADOS,
QUAIS SÃO OS MEUS DIREITOS?

- Confirmação da existência de tratamento
- Acesso aos dados
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta lei
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial
- Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD
- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa
- Revogação do consentimento, nos termos do § 5° do art. 8° da LGPD
- Revisão de decisões automatizadas

5 | Dicas para implementação em estabelecimentos de saúde

5.2 | Como elaborar inventário ou mapeamento de dados pessoais para aplicação da LGPD nos estabelecimentos de saúde

A implementação da LGPD nos estabelecimentos de saúde demanda a elaboração de um documento que elucide, minimamente:

(i) o que o estabelecimento faz com os dados pessoais (desde a coleta até a destruição/eliminação)

(ii) quais dados pessoais são tratados pela empresa

(iii) quais as operações de tratamento a que esses dados são submetidos (os dados são armazenados, são processados, são transmitidos?) e

(iv) quais as medidas de segurança que protegem tais dados pessoais

- o tratamento de dados pessoais, inclui:
- todas as operações feitas em suporte digital
  exemplos: nuvem, mídias, pen drive, CDs, disquetes etc.
- e também o tratamento feito em suporte físico
  exemplos: papel, RX, material genético, moldes de gesso de arcada dentária, lâminas de laboratório etc

9

INVENTÁRIO
- Descrição básica
- "Fotografia" do processo de tratamento dos dados pessoais

MAPEAMENTO
- Descrição completa
- Detalhamento do processo de tratamento dos dados pessoais

5 | Dicas para implementação em estabelecimentos de saúde

5.3 | Termo de Consentimento para Tratamento dos Dados Pessoais

A clínica, consultório laboratório, hospital ou plataforma de seja destina à consultas virtuais, deve elaborar Termo de Consentimento para Tratamento dos Dados Pessoais, que deverá ter o aceite de cada paciente/titular de dados pessoais

Quaisquer meios vituais, digitais, devem seguir as legislações específicas da internet, como o Marco Civil da Internet (Lei 12.965/14) e as recomendações de cada conselho de classe, tais como o Conselho de Medicina, Conselho de Nutrição, Conselho de Psicologia

Essas resoluções dos conselhos devem ir se adaptando às novas formas tecnológicas e realidades cotidianas, tais como ocorrido durante a pandemia da Covid-19

Certo é que prestação de serviço de saúde com padrões digitais deverá seguir os **padrões normativos e éticos usuais do atendimento presencial**, com o custeio da empresa e com formas de remuneração possíveis ao seu tempo

O que deve ter no Termo de Consentimento?	Dados do profissional | Dados do paciente
	Dados da pessoa que marcou a consulta (responsável)
	Definições da teleconsulta e suas limitações
	SEMPRE ter acesso às informações antes de dar consentimento
	ANTES DO ACESSO NO CONSULTÓRIO VIRTUAL
	Política sobre o prontuário do paciente
	Informações sobre o pagamento
Se Crianças e Adolescentes?	Além do geral acima
	Não esquecer do Termo de Consentimento Específico
	DESTACADO
	Linguagem CLARA E ACESSÍVEL
	Com a autorização do responsável
	ANTES DA COLETA DAS INFORMAÇÕES

Sobre Termos de Consentimento

Existe só um tipo de termo de consentimento?

TODOS TEM EM COMUM

- Tem que ser em linguagem clara
- De acordo com o nível de compreensão
- Do paciente e dos acompanhantes
- Tem que ser livre e esclarecido
- Tem que explicar o que ocorrerá
- Tem que ser destacado
- Tem que ser consciente
- Tem que ser facilitado
- Facilitada a experiência do usuário

- Existem vários tipos de consentimento
- CONSENTIR é ACEITAR
- Na área de saúde tem vários tipos conhecidos:
  - Termo de consentimento para um tratamento médico, odontológico, radiológico
  - Termo de consentimento de transfusão de sangue
  - Termo de consentimento de intervenção cirúrgica
  - Termo de consentimento de uso de imagem, de voz
  - Termo de consentimento de tratamento de dados pessoais (pode ser revogado a qualquer tempo)
  - Etc.

5 | Dicas para implementação em estabelecimentos de saúde

5.4 | Segurança, proteção e guarda dos dados

A preocupação com a guarda dos dados pessoais é fundamental, especialmente porque a LGPD dispõe sobre proteção tanto de dados pessoais digitais quanto físicos

Vale dizer, dados pessoais não são apenas os que estão no computador. Os dados pessoais físicos também devem ser tratados

Assim, independe da forma em que se coleta dado pessoal, se está numa planilha excel, sistema operacional específico ou uma ficha impressa, é necessário observar os requisitos de segurança para mitigação (diminuição) de riscos de incidentes

Existem médicos e profissionais da saúde em geral que ainda fazem o prontuário em papel. Não há problema, mas é preciso ter cuidado ao trabalhar com prontuário em papel que está sujeito às regras da LGPD. É possível vazar ao se deixar um prontuário físico em arquivo sem tranca e sendo manuseado por colaborador ou parceiro que não é da área da saúde, isso é considerado um incidente de vazamento de dados pessoais

Para proteger os dados pessoais físicos, os documentos devem ser armazenados em local seguro e restrito, utilizando-se **arquivo ou portas de entrada com chave** e os colaboradores que tenham acesso ter **termos de sigilo** ou **cláusulas de sigilo** nos contratos de trabalho, **realizar treinamentos para comunicação mais discreta** e que se restrinja ao paciente e que não seja escutada na recepção por outros pacientes

Também se revela importante **não permitir** o uso **de pen-drives, HD externos** ou **outros dispositivos desconhecidos** que possam **ocasionar invasões na rede**, com possibilidade maior de incidentes de vazamentos de dados pessoais

Em relação dados pessoais digitais é importante que o servidor, computadores e dispositivos móveis como tablets, ipad, smartphones, tenham antivírus, não utilize softwares e sistema operacional piratas, sejam sempre atualizados, restringindo o acesso com senhas que possuam os requisitos mínimos de segurança, ou seja, contenham letras maiúsculas e minúsculas, números e caracteres especiais, bem como tenham implementado ou implementem gestão de uso do Wi-Fi e Política Interna de Segurança da Informação

Os dispositivos que pertençam aos profissionais da saúde e contenham dados pessoais devem ser **armazenados em local seguro e restrito**, nunca deve ser compartilhado, devendo ser eliminado de forma segura, quando for substituído, observando-se, naturalmente, a temporalidade dos documentos

Sobre Câmeras de Segurança

As clínicas e consultórios devem se preocupar, ainda, com os circuitos internos de câmeras de segurança, exigir a preservação de direitos de terceiros, prestador de serviços contra incidentes de vazamento de dados pessoais ou invasões

O QUE SE DEVE SABER????:

- quem tem acesso às imagens
- se são acessadas pelo celular
- se são gravadas
- quanto tempo ficam gravadas
- softwares e sistemas de proteção utilizados,
- adotando todo cuidado para que as imagens não vazem

As medidas de segurança previstas na LGPD são **técnicas** e **administrativas** aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito

5 | Dicas para implementação em estabelecimentos de saúde

5.4.1 | O que são medidas técnicas?

São medidas voltadas à infraestrutura de rede de Tecnologia da Informação

Tais como:

- Firewall
- Antivírus
- DLP (Data Loss Prevention)
- Uso de senhas fortes
- Acesso à informação
- Atualização de softwares
- Uso de correio eletrônico (e-mail)
- Etc

5.4.2 | O que são medidas administrativas?

São medidas voltadas mais à gestão e estrutura documental

Tais como:

- Políticas de privacidade
- Códigos de conduta
- Políticas de cookies
- Treinamento
- Acordo de confidencialidade para colaboradores e terceiros que tratam dados pessoais
- Foco cultura de proteção de dados

DESTAQUE

No tratamento de **dados pessoais sensíveis**, as medidas de segurança deverão ter um **cuidado especial**, prevendo salvaguardas e mecanismos de mitigação (diminuição) de riscos

5 | Dicas para implementação em estabelecimentos de saúde

5.5 | Compartilhamento de dados com outros médicos e profissionais de saúde

Quando o profissional de saúde se depara com um caso raro e deseja ouvir outras opiniões ou apresentar o caso em grupo de estudos ou em congresso da especialidade, o **compartilhamento da informação somente será possível sem a identificação do paciente**. Caso contrário, sugere-se a coleta de consentimento do paciente para autorizar o compartilhamento de forma específica

No que se refere a troca de informações pessoais entre médicos/profissionais de saúde e seus pacientes por meio de canais de comunicação como WhatsApp, Telegram, e-mail e outras plataformas eletrônicas, importante se atentar ao fato de que informações **podem ser transmitidas apenas para o próprio titular** ou a quem o mesmo tiver autorizado formalmente (Exemplo: termo de autorização para terceiro) ou legalmente (Exemplo: pais de um menor, tutor de um incapaz, etc.)

Ademais, deve SEMPRE ser preservada a **intimidade e a privacidade** do titular de dados pessoais, **não sendo recomendável** a utilização de plataforma pública para troca de informações pessoais ao paciente, sendo necessário, ainda, que os canais eletrônicos utilizados para estas comunicações possuam requisitos de segurança e preferencialmente criptografia de ponta a ponta

Sugere-se, ainda, que após finalizar o contato, não havendo necessidade de armazenamento, as mensagens sejam **imediatamente excluídas**, minimizando os riscos de incidentes de vazamento de dados

A LGPD proíbe a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica

5 | Dicas para implementação em estabelecimentos de saúde

5.6 | Dado anonimizado

Dado anonimizado é dado relativo a **titular que não possa ser identificado**, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Pseudoanonimizado pode ser revertido, dificulta a vinculação direta, mas é possível ser revertido em dado pessoal comum.

IMPORTANTE
Danos anonimizados não são objeto de aplicação da LGPD, uma vez que não são relacionados ao seu titular. Exemplo: Dados estatísticos em pesquisas de saúde publica

DADOS SEM ANONIMIZAR

CPF	Nome	Idade	Sexo	Mês	CID
123.456.7890	João da Silva	45	M	Outubro	123
098.765.4321	Antônio Pedro	56	M	Outubro	123
999.888.7776	Maria Jose	45	F	Outubro	454
888.777.6665	Luisa Pedroso	56	F	Outubro	454
777.999.8887	Martha da Silva	48	F	Outubro	454
124.324.4443	Silvio Silas	48	M	Outubro	454

DADOS PSEUDO ANONIMIZADOS

CPF	Nome	Idade	Sexo	Mês	CID
123.***.**90	J*** d* S****	45	M	Outubro	123
098.***.**21	A****** P****	56	M	Outubro	123
999.***.**76	M**** J***	45	F	Outubro	454
888.***.**65	L**** P******	56	F	Outubro	454
777.***.**87	M***** d* S****	48	F	Outubro	454
124.***.**43	S***** S****	48	M	Outubro	454

DADOS ANONIMIZADOS

CPF	Nome	Idade	Sexo	Mês	CID
		45	‘	Outubro	123
		56	M	Outubro	123
		45	F	Outubro	454
		56	F	Outubro	454
		48	F	Outubro	454
		48	M	Outubro	454

Observe que os campos que identificam a pessoa natural (CPF, Nome) passaram por um processo que dificulta a sua identificação. Os demais dados tratados (Idade, sexo, mês e CID) podem ser utilizados de forma estatística

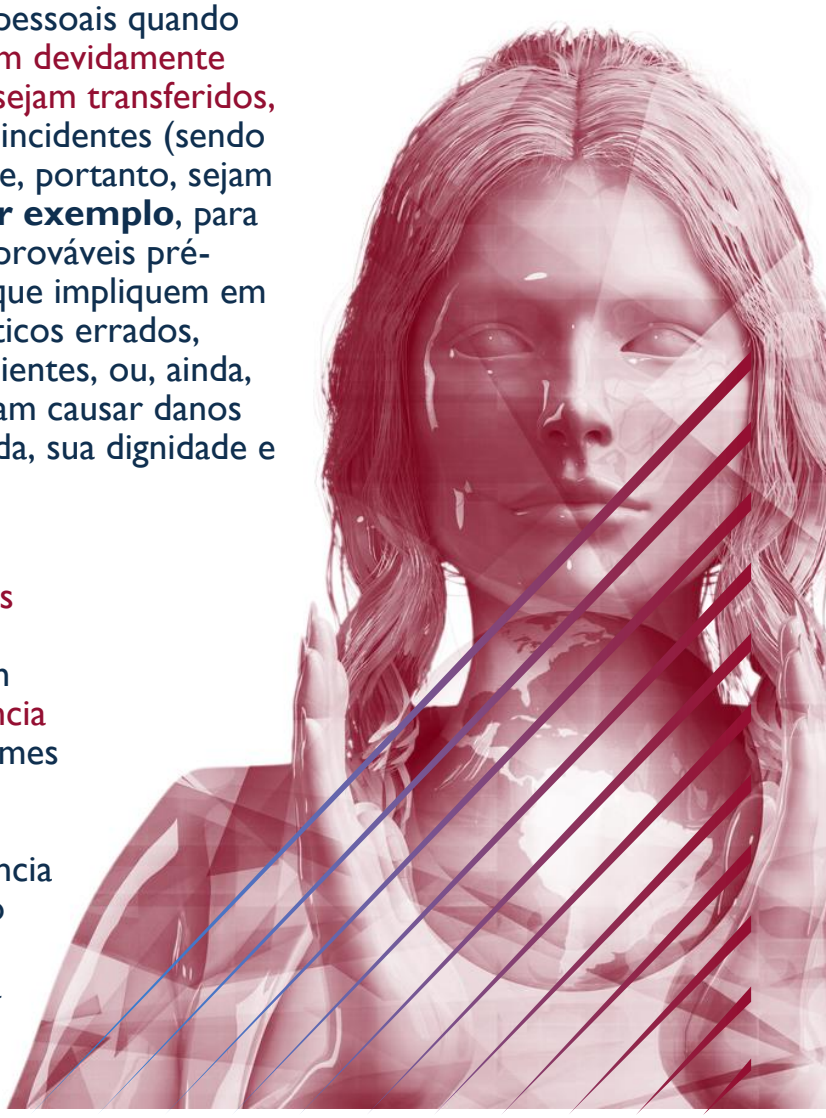
Exemplo: 4 pessoas abaixo de 50 anos, 2 pessoas acima de 50 anos, 3 homens e 3 mulheres, 2 CID 123 e 4 CID 454. Neste formato não se identifica diretamente (CPF) ou indiretamente (característica única)

6 | Utilização ética dos dados pessoais na inteligência artificial no setor de saúde

A Inteligência Artificial utiliza bancos de dados para que sua programação algorítmica possa atingir resultados

Imprescindível que toda a utilização de bancos de dados de exames, prontuários e demais documentos contendo dados pessoais - físicos que serão digitalizados; ou que tenham seus dados inseridos em sistemas, bem como dados digitalizados diretamente -, sejam devidamente protegidos, vez que se tratam de dados sensíveis

Importa frisar, ainda, que tais dados pessoais quando utilizados por Inteligência Artificial sejam devidamente tratados e armazenados, evitando que sejam transferidos, manipulados ou que sejam passíveis de incidentes (sendo assim viável a anonimização) de dados, e, portanto, sejam utilizados de forma indevida, como, **por exemplo**, para averiguação de possíveis, mas não comprováveis pré-existências médicas ou outros fatores que impliquem em majoração de planos de saúde, diagnósticos errados, tratamentos que não beneficiem os pacientes, ou, ainda, informações que em mão erradas possam causar danos diretos aos pacientes ou colocar sua vida, sua dignidade e personalidade expostos



Desse modo, a correta adequação, boas práticas de compliance, treinamento e tratamento dos dados para inserção em bancos de dados pessoais para Inteligência Artificial devem estar conforme os ditames da Lei Geral de Proteção de Dados, do sigilo, da ética e dos princípios que a privacidade defende para que a Inteligência Artificial possa ser útil e eficiente como ferramenta de auxílio às instituições médicas e aos profissionais da medicina

7 | Casos práticos

Situações constatadas no cotidiano e a sugestão ofertada

1. CLÍNICAS E CONSULTÓRIOS

Prontuário médico/profissionais da saúde armazenado em armário na recepção, com guarda feita pela recepcionista; profissional da saúde deixar documentos em cima da mesa da recepção; recepcionista manusear prontuário para verificar qual o procedimento que será realizado pelo profissional

ORIENTAÇÃO - não deixar prontuários ou outros documentos de pacientes expostos no balcão; não permitir acesso pela recepcionista aos prontuários; buscar um software para armazenar os dados pessoais com segmentação e senhas de acesso individualizadas. Atenção à segurança física do consultório.

2. CASO DA FARMÁCIA EM MATO GROSSO

A rede Raia/Drogasil, foi multada pelo Procon no importe de R$572.680,71 por realizar coleta de dados pessoais sensíveis (digital) sem esclarecer de forma clara a sua finalidade

Comprovado pela fiscalização que estavam realizando o pedido de consentimento dos consumidores para tratamento, uso e compartilhamento dos dados pessoais, sem que os mesmos tivessem total conhecimento sobre o que estavam autorizando

Não ficou demonstrado o **principal objetivo da coleta e tão pouco a forma clara** e adequada do tratamento dos dados pessoais

(fonte: http://www.procon.mt.gov.br/-/17501890-procon-estadual-multa-rede-de-farmacias-por-infracao-a-lei-de-protecao-de-dados-pessoais?inheritRedirect=true)

Cumpre destacar que, no Estado de SP existe a Lei 17.301 de 01 de dezembro de 2020, que proíbe farmácias e drogarias de exigir CPF do consumidor, sugerimos a leitura da lei:

> *"Proíbe farmácias e drogarias de exigir o CPF do consumidor, no ato da compra, sem informar de forma adequada e clara sobre a concessão de descontos, no Estado, e dá outras providências"*

7 | Casos práticos

Situações constatadas no cotidiano e a sugestão ofertada

3. COMPUTADOR CORPORATIVO

Que não faz impressão e o colaborador envia arquivo para outro computador para imprimir e o descarte realizado de forma incorreta

ORIENTAÇÃO - Neste caso ideal É elaborar uma política de descarte para esses documentos que são impressos. Orientar e treinar sempre os colaboradores da importância do sigilo e descarte. Importante observar também, a política de privacidade da empresa, pois, se o dispositivo não imprime, talvez tenha também algum motivo para isso. Há julgados de demissões por justa causa de colaboradores que descumpriram as regras de uso e sigilo da empresa. Deste modo importante desenvolver sempre a cultura da proteção de dados pessoais e conscientização de todos os colaboradores da instituição

4. CULTURA DA MESA LIMPA OU TELA LIMPA

Quando utilizar computador corporativo é necessário que tenha senha de uso pessoal

ATENÇÃO!! Nunca deixar a senha em um post-it colado no computador. Sendo assim, quando for sair da frente do computador, seja para tomar café ou almoçar, o computador deve ser desligado, nunca deixar a tela aberta com os dados pessoais dos clientes, nem tão pouco papéis sobre a mesa, principalmente contendo informações de pacientes com grande quantidade de dados de saúde. Isso é a cultura da tela limpa e mesa limpa

5. TELEFONE CORPORATIVO DO PROFISSIONAL DA SAÚDE

É de suma importância ter o telefone pessoal separado do corporativo, necessitando de uma política de uso, definir o tipo de informações que podem ser recebidas; quais informações serão passadas para o prontuário do paciente, em quanto tempo serão passadas essas informações para o prontuário; quando serão descartadas, apagadas do dispositivo, para garantir, assim, a segurança dos dados pessoais tratados

7 | Casos práticos

Situações constatadas no cotidiano e a sugestão ofertada

6. DEVE A EMPRESA REALIZAR TESTES DE SEGURANÇA DA INFORMAÇÃO.

SUGESTÃO - Realizar testes, enviando e-mail para verificar se o colaborador está atento às regras de segurança e clica ou não no link enviado. Se houver cliques indevidos, submeter o colaborador a novo treinamento

- Esses são apenas alguns exemplos para que todos possamos refletir sobre os incidentes que porventura possam ocorrer e que medidas devem ser seguidas em conformidade com a política de privacidade criada pela instituição
- Prevenir sempre é o melhor caminho
- Investir na cultura de privacidade de dados pessoais
- Investir nos colaboradores
- Investir na adequação por profissionais especialistas

8 | Descumprimento da Lei

Havendo descumprimento da LGPD, os agentes de tratamento (controlador e operador) de dados pessoais ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional (ANPD), previstas em seu art. 52

Destacamos: As sanções previstas na LGPD são administrativas, portanto, existe a possibilidade de responsabilização por danos na esfera judicial

Penalidades	
	Advertência, com indicação de prazo para adoção de medidas corretiva;
	Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração
	Multa diária, observado o limite total a que se refere o item acima
	Publicização da infração após devidamente apurada e confirmada a sua ocorrência
	Bloqueio dos dados pessoais a que se refere a infração até a sua regularização
	Eliminação dos dados pessoais a que se refere a infração
	Suspensão parcial do funcionamento do banco de dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador
	Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período
	Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados

As multas aplicadas pela ANPD serão destinadas ao Fundo de Defesa de Direitos Difusos que tem por finalidade a reparação dos danos causados ao meio ambiente, ao consumidor, a bens e direitos de valor artístico, estético, histórico, turístico, paisagístico, por infração à ordem econômica e a outros interesses difusos e coletivos

Deve-se ainda observar que o tratamento indevido e sua publicização poderá acarretar prejuízo direto à imagem da organização e sua decorrente perda de clientes e negócios, **talvez em valor superior às multas estabelecidas**

8 | Descumprimento da Lei

A ANPD publicou em 28.10.2021, sua primeira Resolução CD/ANPD nº 1, sobre o regulamento do processo de fiscalização e processo administrativo sancionador.

Agente regulados, agentes de tratamento e demais integrantes ou interessados no tratamento de dados pessoais (art. 4º, I)

Autuado, agente regulado que, com indícios suficientes infração, tem instaurado processo administrativo sancionador, por meio de auto de infração (art, 4º, II)

Denúncia, comunicação à ANPD por qualquer pessoa, natural ou jurídica, de suposta infração cometida contra LGPD, que não seja uma petição de titular (art, 4º, III)

Obstrução à atividade de fiscalização, por ação ou omissão, direta ou indireta, da fiscalização, que impeça, dificulte ou embarace a atividade de fiscalização pela ANPD, com entrave à situação dos agentes, a recusa no atendimento, e o não envio ou envio intempestivo de quaisquer dados e informações pertinentes à obrigação do agente regulado (art. 4º, IV)

Petição titular, comunicação feita à ANPD pelo titular de dados pessoais de uma solicitação apresentada ao controlador e não solucionada no prazo estabelecido em regulamentação, nos termos do inciso V do art. 55-J da LGPD (art, 4º, V)

Requerimento conjunto de tipos de comunicação, compreendendo a petição de titular e a denúnci(art. 4º, VI)

Definições principais

Deveres agentes regulados

Destacamos: Quanto mais boas práticas forem adotadas, melhor será a análise dos processos da ANPD

Fornecer cópia de documentos, físicos ou digitais, dados e informações relevantes para a avaliação das atividades de tratamento de dados pessoais, no prazo, local, formato e demais condições estabelecidas pela ANPD (art. 5º, I)

Permitir o acesso às instalações, equipamentos, aplicativos, facilidades, sistemas, ferramentas e recursos tecnológicos, documentos, dados e informações de natureza técnica, operacional e outras relevantes para a avaliação das atividades de tratamento de dados pessoais, em seu poder ou em poder de terceiros (art. 5, II)

Possibilitar que a ANPD tenha conhecimento dos sistemas de informação utilizados para tratamento de dados e informações, bem como de sua rastreabilidade, atualização e substituição, disponibilizando os dados e as informações oriundos destes instrumentos (art. 5º, III)

Submeter-se a auditorias realizadas ou determinadas pela ANPD (art. 5º, IV)

Manter os documentos físicos ou digitais, os dados e as informações durante os prazos estabelecidos na legislação e em regulamentação específica, bem como durante todo o prazo de tramitação de processos administrativos nos quais sejam necessários (art. 5º, V)

Disponibilizar sempre que requisitado, representante apto a oferecer suporte à atuação da ANPD, com conhecimento e autonomia para prestar dados, informações e outros aspectos relativos a seu objeto (art. 5º, VI)

8 | Descumprimento da Lei

Resolução CD/ANPD nº 1
Processo de fiscalização
Processo administrativo sancionador

Aplicação de sanções por meio de processo administrativo sancionador. Compõe a atividade repressiva da ANPD. Poderá ser instaurado de ofício. Em decorrência de processo de monitoramento, de requerimento, após efetuar análise de admissibilidade.

Procedimento preparatório poderá tramitar em sigilo e efetuar averiguações preliminares. Quando há indícios suficientes para instauração imediata do processo administrativo sancionador. Poderá realizar diligências. Conclusão pelo arquivamento ou pela instauração de processo administrativo sancionador

Termo de ajuste de conduta (TAC) a o interessado poderá apresentar proposta de celebraçao de TAC. Processo sancionatório será suspenso após a assinatura do termo, e arquivado cumprimento integral, terá regulamentação própria

Fases de Instauração e de instrução a lavratura do auto de infração, defesa do autuado, pedido de produção de prova pericial, alegações finais, relatório da instrução

Fase de decisão 1ª instância, motivada, fatos e fundamentos jurídicos e sanção

Fase de recurso ao Conselho Diretor da ANPD, pode ter efeito suspensivo. Juízo de reconsideração, relatoria e julgamento do recurso.

Do cumprimento da decisão e da inscrição na Dívida Ativa e da Revisão, se houver fatos novos

Fiscalização, que é objeto da atuação responsiva, são atividades de monitoramento, orientação, atuação preventiva e atividade represiva, conforme os procedimentos do Regulamento

Meios de atuação, de ofício, em decorrência de programas periódicos de fiscalização, de forma coordenada com órgãos e entidade públicos, ou em cooperação com autoridades de proteção de dados pessoais de outros países

Fiscalização promoverá o conhecimento das normas e políticas públicas sobre proteção de dados pessoais e medidas de segurança, de forma a disseminar boas práticas

Medidas de orientação, o conhecimento elaboração e disponibilização de guias de boas práticas, de ferramentas de autoavaliação de conformidade e de riscos, modelos de documentos para serem utilizados, sugestção de realização de treinamentos e cursos, reconhecimento e divulgação das regras de boas práticas e de governança, recomendação de utilização de padrões tecnicos e implementação de programa de governança em privacidade

Medidas preventivas divulgação de informações, aviso, solicitação de regularização ou informe e plano de confirmidade.

9 | Saiba mais...

A QUEM NÃO SE APLICA A LGPD? A LGPD não se aplica para fins exclusivamente jornalísticos e artísticos; de segurança pública; de defesa nacional; de segurança do Estado; de investigação e repressão de infrações penais; particulares (ou seja, a lei só se aplica para pessoa física ou jurídica que gerencie bases com fins ditos econômicos). E não se aplica aos dados que se encontram fora do Brasil e que não sejam objeto de transferência internacional

PRINCÍPIOS DA LGPD Conforme art. 6° as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I – finalidade; II – adequação: III – necessidade; IV - livre acesso; V - qualidade dos dados; VI – transparência; VII – segurança; VIII – prevenção; IX - não discriminação e X - responsabilização e prestação de contas

Princípios da LGPD	
	Finalidade é a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades
	Adequação é a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento
	Necessidade é a limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados
	Livre acesso é a garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais
	Qualidade dos dados é a garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento
	Transparência é a garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial
	Segurança é a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
	Prevenção é a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais
	Não discriminação impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos
	Responsabilização e prestação de contas é a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas

10 | Considerações finais

A **finalidade da Lei não é proibir** a utilização dos dados pessoais, mas **sim trazer regras** de acesso e cuidados nos procedimentos de manipulação e guarda, respeitando os direitos dos titulares de, saber porque são coletados, de que forma são utilizados e como serão descartados os seus dados, seguindo o princípio da boa-fé e da transparência na relação interpessoal

O propósito desta cartilha é trazer informações a respeito das determinações da Lei Geral de Proteção de Dados, com situações práticas e relevantes para o processo e governança em proteção de dados pessoais, seguindo os princípios e as bases legais, principalmente relacionadas aos dados pessoais sensíveis e de saúde que são os mais utilizados em consultórios de profissionais de saúde

Deste modo, seguir as orientações, buscando sempre atender os princípios, direitos e garantias fundamentais dos titulares de dados pessoais, **trará segurança** na relação entre controladores, operadores e titulares de dados pessoais, onde a compreensão, a conscientização na proteção dos dados pessoais deve ser observada e tratada com zelo por todos os envolvidos na relação

Mitigar riscos e evitar demanda judiciais **só depende de cada um**, pois as regras foram estabelecidas pela lei e devem ser seguidas. Esperamos que aproveitem ao máximo as informações que foram trazidas e as utilizem com zelo

A prevenção e boas condutas são um ótimo investimento com retorno pela redução de custos com eventuais penalidades

11 | Documentos de apoio para adequação a LGPD

Publicações da ANPD.

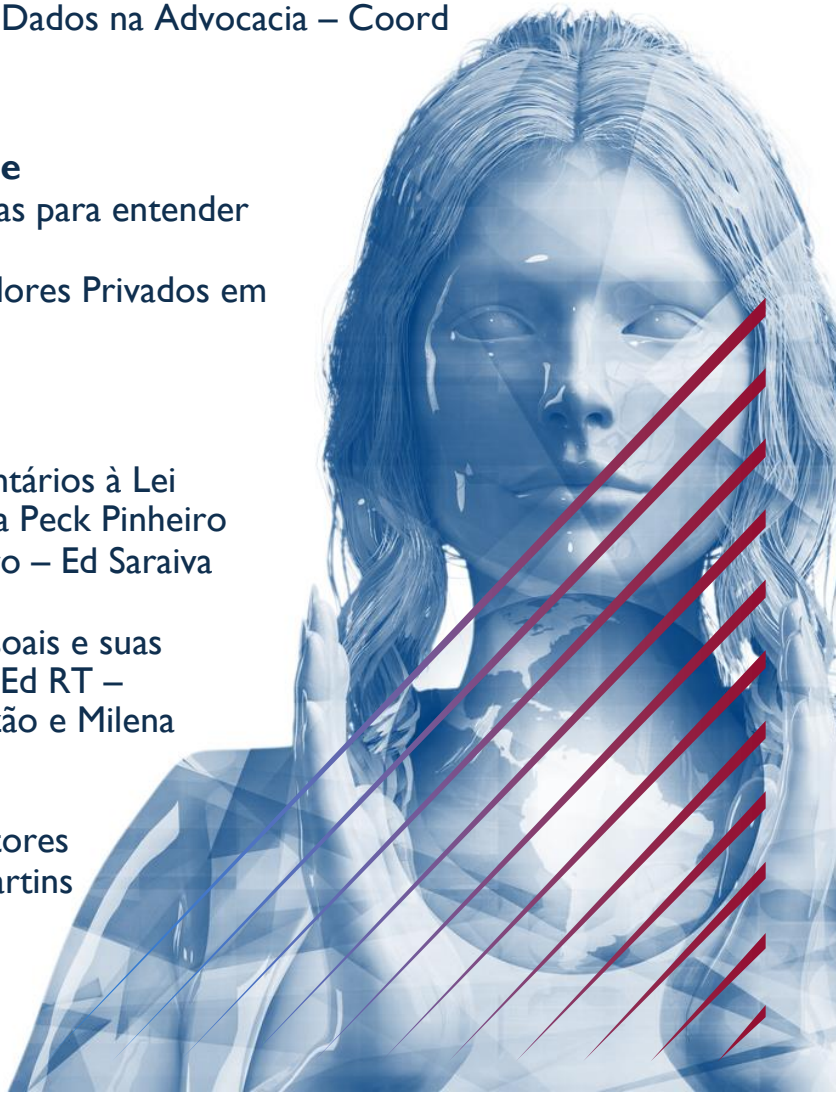
- Segurança da Informação para Agentes de Tratamento de Pequeno Porte (Guia Orientativo) – (checklist medidas de segurança)
- Definições sobre Agentes de Tratamento de Dados Pessoais e do Encarregado (Guia Orientativo)
- Como Proteger seus Dados Pessoais (Guia do Consumidor)
- Vazamento de Dados (Fascículo Cert.br)
- Proteção de Dados (Fascículo Cert.br)

Cartilhas da Comissão de Privacidade e Proteção de Dados Pessoais da OAB/SP

- Incidentes de Segurança– Coord Educação (Cartilha)
- Boas Práticas de Proteção de Dados na Advocacia – Coord Educação (Cartilha)

Cartilhas de setores da saúde

- ANS – LGDP Informações básicas para entender (Cartilha)
- Proteção de Dados para Prestadores Privados em Saúde (Código de Boas Práticas)



Sugestões Bibliográficas.

- Proteção de Dados Pessoais - Comentários à Lei 13709/2018 – Ed Saraiva Jur – Patricia Peck Pinheiro
- Direito Digital – Patrícia Peck Pinheiro – Ed Saraiva Jur
- Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro – Ed RT – Coords. Gustavo Tepedino, Ana Frazão e Milena Donato Oliva
- Proteção de Dados na Saúde: Manual prático da LGPD para médicos e gestores
- por Amanda Cunha e Mello Smith Martins e André Gebara Königsberger
- LGPD - Lei Geral De Proteção De Dados Pessoais Manual De Implementação – Ed RT – Coord Viviane Nóbrega Maldonado

LGPD PARA CONSULTÓRIOS
ÁREA DA SAÚDE

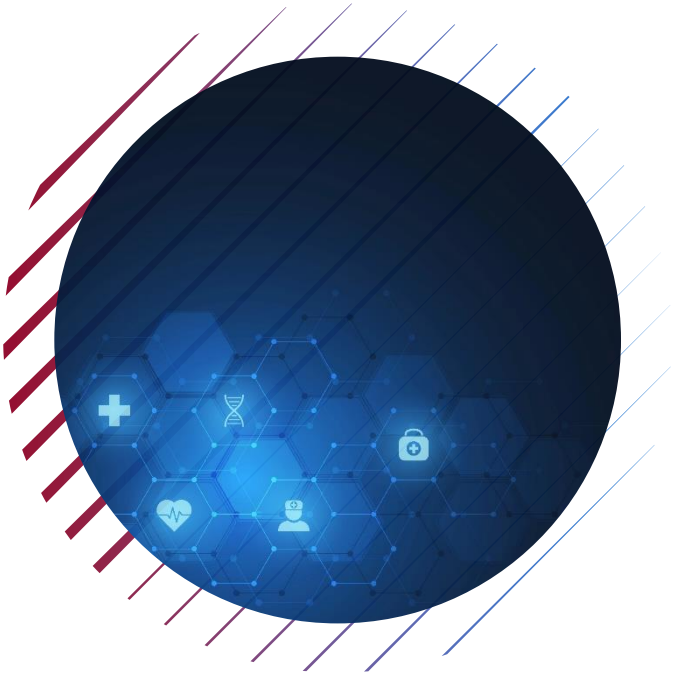
Coordenadora do grupo:
Maria Cristina Gonçalves

Colaboradores da Cartilha:
Caren Viani, Fabiana dos Santos Medeiros, Greycielle Amaral, Isabella Rainho, Marcelo Fonseca Santos, Marcus Vinícius Ramos, Maria Cristina Fleming, Maria Cristina Gonçalves, Nilton Nascimento Ramos, Priscilla Tricate, Rosália Toledo Veiga Ometto, Valéria de Almeida Franco e Victor Machado.

Revisão de texto:
Greycielle Amaral

Edição e Arte:
Rosália Toledo Veiga Ometto

Realização:
Coordenação da Saúde da Comissão Especial de Privacidade e Proteção de Dados da OAB/SP.



Diretoria Executiva Comissão Especial de Privacidade e Proteção de Dados da OAB/SP:
Patrícia Peck Pinheiro – Presidente
Marcelo Lapolla – Vice-Presidente
Marcelo Crespo – 1° Secretário
Gabriela De Ávila Machado – 2ª Secretária