IPACOM
Instituto Paranaense de Compliance

Guia 05
LGPD na Saúde - Aspectos Legais e Regras Específicas Para o Setor

IPACOM
Instituto Paranaense de Compliance

Este guia foi elaborado pelos membros do Grupo de Trabalho de LGPD do Instituto Paranaense de Compliance (IPACOM)

Elaboração
Ana Paula Aleixo
Camilla M. Ribas da Silva
Marizete Figueiredo

Coordenação
Letícia Sugai

Sistemas de Saúde do País

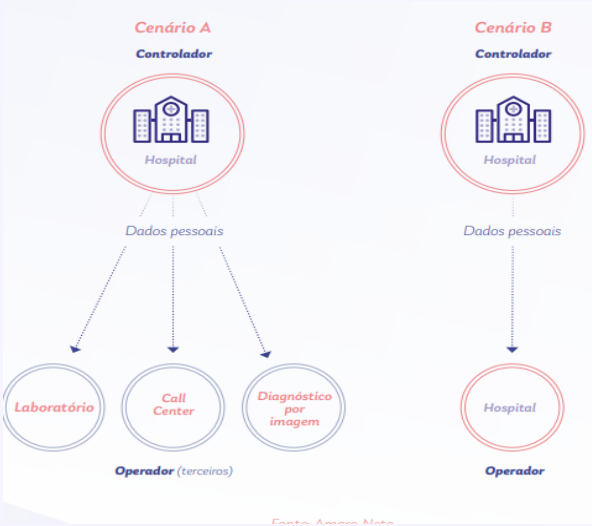
O Sistema Nacional de Saúde é composto por 3 grandes grupos, os quais possuem seus órgãos normativos acerca dos dados compartilhados:

- **SUS** – Sistema Único de Saúde – Ministério da Saúde (MS)
- **Saúde Complementar** – Agência Nacional de Saúde Complementar (ANS)
- **Saúde Privada** – Conselho Federal de Medicina

Controlador e Operador

- **Controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

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



IPACOM
Instituto Paranaense de Compliance

DADOS – art. 5º Lei 13709/18 LGPD

- Dados Pessoais: informações relacionadas a pessoa natural identificada ou identificável
- Dados sensíveis: dado pessoal sobre 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

O dado referente à área da saúde é classificado como DADO SENSÍVEL, mas também existem os dados pessoais e seu tratamento pode ocorrer de duas formas, conforme art. 7º e 11 da LGPD:

I. Com o consentimento do titular
II. Sem o consentimento do titular, desde que indispensável para determinadas hipóteses.

Responsabilidade

- Os dados pessoais a serem tratados na área da saúde podem se enquadrar nas hipóteses onde o consentimento em si não é obrigatório.

- Sob essas hipóteses os dados podem ser tratados sem o consentimento do titular, contudo deverá se dar na forma da lei, pois a eventual dispensa não desobrigada os agentes de tratamento das demais obrigações previstas na Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular. (artigo 7º, §6º).

IPACOM
Instituto Paranaense de Compliance

Ciclo de vida de dados LGPD

IPACOM
Instituto Paranaense de Compliance

Consentimento – art. 11, I, Lei 13709/18 LGPD

- Art. 5º, XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
- Art. 8, § 4º - O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

Caso haja necessidade de obter o consentimento para tratamento de dados sensíveis, o titular deverá ter acesso a informações mínimas, tais como:

- Finalidade do tratamento de dados
- Forma e duração do tratamento
- Identificação do controlador
- Informações se os dados serão compartilhados

✓ Isso evidencia a necessidade de descrição das finalidades específicas, pois caberá ao controlador comprovar que o consentimento foi obtido de forma regular e foram respeitados os preceitos da LGPD (art. 8, §2°)

IPACOM
Instituto Paranaense de Compliance

Hipóteses que o consentimento é dispensável – art. 11, II, LGPD Aplicação na saúde

A LGPD previu 6 possibilidade para tratamento de dados sensíveis sem o consentimento, desde que comprovado que a coleta do dados foi indispensável. Alguns são específicos para a área de saúde:

I - Cumprimento de obrigação legal ou regulatória pelo controlador
EX1: notificação compulsória: o Ministério da Saúde estipula uma lista de doenças ou agravos em que é obrigatória a comunicação pelos serviços públicos e privados e a autoridade da saúde poderá divulgar esses dados. Isso acontece com a COVID-19, conforme Portaria nº 356/MS os resultados dos exames precisam ser notificados por laboratórios públicos e privados para controle epidemiológico.

EX2: No Sistema de Informações de Beneficiários, mantido pela ANS, em que as Operadoras informam os dados cadastrais dos beneficiários, migração de planos, etc, para que a ANS avalie situações de mercado (Resolução normativa 295/2012).

EX3: Para cadastro do CNES (Cadastro Nacional de Estabelecimento de Saúde), a administração pública exige uma série de informações relacionadas ao estabelecimento e seus funcionários.

IPACOM
Instituto Paranaense de Compliance

Hipóteses que o consentimento é dispensável – art. 11, II, Lei 13709/18 LGPD

II - Execução de Políticas Públicas
Não há uma definição específica sobre o que pode ser considerado política pública, o que deixa a aplicabilidade ampla especialmente quando a ação é aplicada pela própria Administração pública, o que necessitará de orientações e normativos pela ANPD.
EX: Parcerias para oferta de medicamentos

III - Realização de estudos por Órgãos de Pesquisa
EX: pesquisas clínicas envolvendo seres humanos estão regulamentadas pela Resolução 466 do Conselho Nacional de Saúde, que trazem conceitos também previstos na LGPD, como a garantia de sigilo e da privacidade dos participantes.

IV - Exercício Regular de Direitos
Garante o compartilhamento de dados sensíveis inclusive para exercício de direito previsto em contrato, processo judicial ou arbitral.
EX: não é necessário o consentimento do titular para fornecer seus dados coletados pelo hospital, quando este tem contrato de prestação de serviços com o laboratório que irá realizar seu exame.

Hipóteses que o consentimento é dispensável – art. 11, II, Lei 13709/18 LGPD

V - Proteção da vida ou da incolumidade física do titular ou de terceiro
EX1: necessidade de tratamento de dados pela Administração Pública para salvar vidas em uma situação de catástrofe.
EX2: utilização de informações para prevenção, investigação e repressão de infrações penais pelos agentes públicos responsáveis pela vida de terceiros.

VI - Tutela da Saúde
Será dispensável o consentimento para tratamento de dados quando for utilizado por profissional da saúde, serviço de saúde ou autoridade sanitária quando indispensável para tutela da saúde.
Torna-se necessário que a ANPD traga esclarecimentos sobre o conceito de "tutela da saúde" para deixar o tema menos amplo e trazer maior segurança jurídica.

IPACOM
Instituto Paranaense de Compliance

Compartilhamento de dados da saúde – art. 11, §4º Lei 13709/18 LGPD

Fins econômicos
É proibido a comunicação ou compartilhamento de dados sensíveis da saúde com o objetivo de obter vantagem econômica, exceto para:
- ✓ Prestação de serviços da saúde
- ✓ Assistência farmacêutica
- ✓ Assistência à saúde

EX: possibilidade de compartilhamento de dados entre Operadoras, prestadores de serviços e Gestores do SUS

Observações importantes
- ✓ O compartilhamento deve estar atrelado ao interesse do titular
- ✓ Proibida a prática de compartilhamento para seleção de riscos na contratação e exclusão de beneficiários (EX: troca de informações entre farmácias e Operadoras para consultar os tipos de medicamentos que o titular toma antes de aceita-lo)

IPACOM
Instituto Paranaense de Compliance

Atenção especial ao Setor de Saúde

- Crianças e adolescentes (menores de 18 anos): informações poderão ser coletadas somente com autorização dos pais ou responsáveis
- Cuidados especiais com placas de identificação nos quartos e leitos de hospitais
- Maior fiscalização em prontuários físicos ou virtuais para evitar vazamento

IPACOM
Instituto Paranaense de Compliance

Medidas e Ações

IPACOM
Instituto Paranaense de Compliance

Medidas e Ações

Assistencial e corpo clínico:

Não emprestar credenciais;

Não salvar informações localmente ou em meios que não sejam controlados pela instituição;

Não compartilhar informações confidenciais por aplicativos de mensagens instantâneas, redes sociais, e-mail particular ou qualquer outro que não exista controle da instituição;

Aderir às políticas de privacidade e tomar todas as cautelas necessárias no manuseio de dados sensíveis;

Não conversar em locais públicos mencionando dados sensíveis de pacientes.

Gestão de fornecedores/contratos:

Aplicar os termos desenvolvidos pelo jurídico para novos contratos e criar aditivos para os contratos já existentes;

Auditoria periódica nas operadoras e prestadores de serviço onde exista a transferência de informações que contenham dados pessoais.

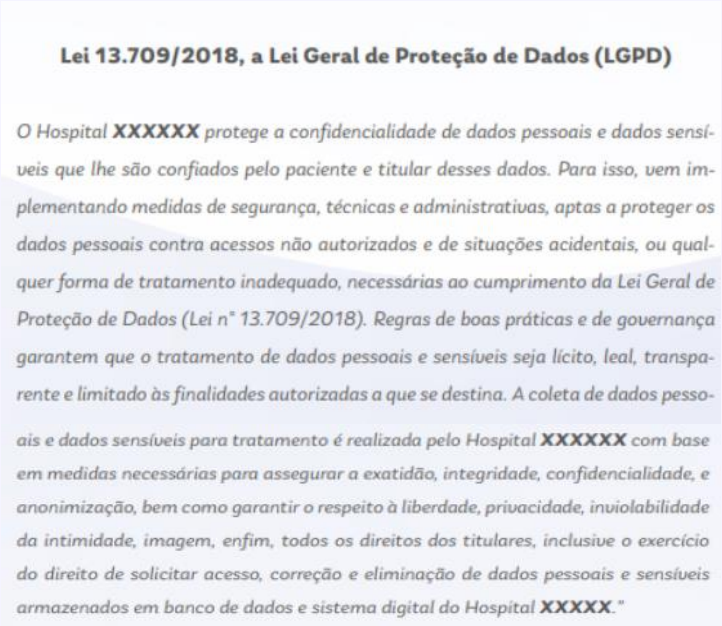
IPACOM
Instituto Paranaense de Compliance

Medidas e Ações

Tecnologia da Informação e Segurança da Informação:

- Desenvolver meios seguros de armazenamento, processamento e transmissão para proteção de dados pessoais;
- Desenvolver e divulgar as Políticas de Segurança da Informação, incluindo Política de Classificação da Informação;
- Levantar e documentar as interfaces de troca de informações com dados sensíveis (arquiteto de dados);
- Segregar perfis de acesso a dados pessoais e gestão de acessos;
- Proteger contra vazamento de informação, bloqueio de pendrive e DLP Endpoint para as estações de trabalho;
- Cybersecurity (Monitoração, alerta, segregação de ambientes);
- Definir de tecnologias para gestão dos termos de consentimento de pacientes e colaboradores para uso dos dados (método de armazenamento, pesquisa, tratamento dos casos de não consentimento, revogação/mudança do consentimento, exclusão de dados);
- Definir de tecnologias para processo de transferência segura de dados sensíveis (operadoras nacionais e internacionais);
- Definir anonimização e pseudonomização em banco de dados;
- Assegurar continuidade de negócios (possibilidade de multa em caso de perda de informação do paciente);
- Conscientizar os colaboradores e prestadores de serviço;
- Desenvolver processo seguro que envolva testes durante todo o ciclo.

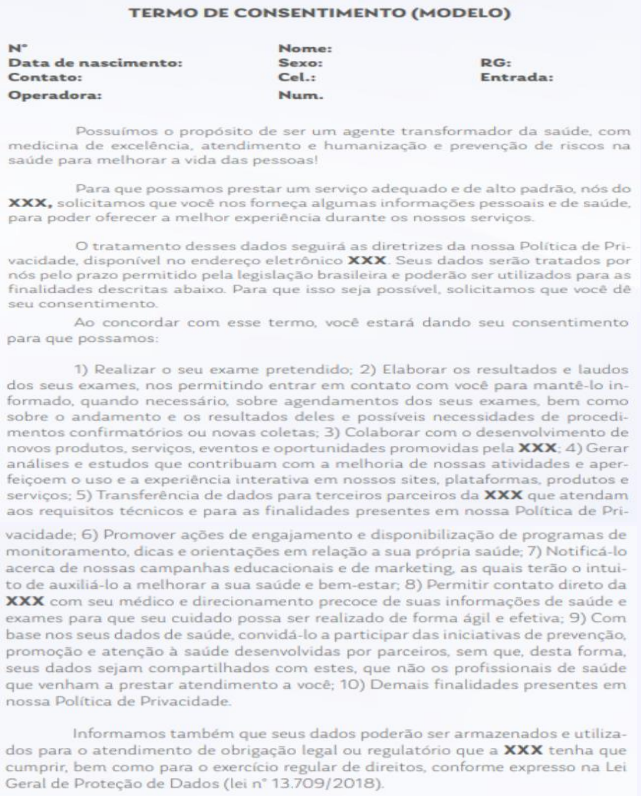
O desenvolvimento da Política de Segurança da Informação, Política de Gestão de Mudanças, política de uso de e-mail, política de uso de internet, entre outras, faz parte das ações de construção de diretrizes promovidos pelas organizações, na busca de incutir regras seguras em seus colaboradores.



Lei 13.709/2018, a Lei Geral de Proteção de Dados (LGPD)

*O Hospital **XXXXXX** protege a confidencialidade de dados pessoais e dados sensíveis que lhe são confiados pelo paciente e titular desses dados. Para isso, vem implementando medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais contra acessos não autorizados e de situações acidentais, ou qualquer forma de tratamento inadequado, necessárias ao cumprimento da Lei Geral de Proteção de Dados (Lei nº 13.709/2018). Regras de boas práticas e de governança garantem que o tratamento de dados pessoais e sensíveis seja lícito, leal, transparente e limitado às finalidades autorizadas a que se destina. A coleta de dados pessoais e dados sensíveis para tratamento é realizada pelo Hospital **XXXXXX** com base em medidas necessárias para assegurar a exatidão, integridade, confidencialidade, e anonimização, bem como garantir o respeito à liberdade, privacidade, inviolabilidade da intimidade, imagem, enfim, todos os direitos dos titulares, inclusive o exercício do direito de solicitar acesso, correção e eliminação de dados pessoais e sensíveis armazenados em banco de dados e sistema digital do Hospital **XXXXX**."*

O consentimento deve ser obtido em conformidade com a lei, que em seu artigo 5º XII define: “Para os fins dessa lei considera-se: Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”.



TERMO DE CONSENTIMENTO (MODELO)

Nº	**Nome:**	
Data de nascimento:	**Sexo:**	**RG:**
Contato:	**Cel.:**	**Entrada:**
Operadora:	**Num.**	

Possuímos o propósito de ser um agente transformador da saúde, com medicina de excelência, atendimento e humanização e prevenção de riscos na saúde para melhorar a vida das pessoas!

Para que possamos prestar um serviço adequado e de alto padrão, nós do **XXX,** solicitamos que você nos forneça algumas informações pessoais e de saúde, para poder oferecer a melhor experiência durante os nossos serviços.

O tratamento desses dados seguirá as diretrizes da nossa Política de Privacidade, disponível no endereço eletrônico **XXX**. Seus dados serão tratados por nós pelo prazo permitido pela legislação brasileira e poderão ser utilizados para as finalidades descritas abaixo. Para que isso seja possível, solicitamos que você dê seu consentimento.

Ao concordar com esse termo, você estará dando seu consentimento para que possamos:

1) Realizar o seu exame pretendido; 2) Elaborar os resultados e laudos dos seus exames, nos permitindo entrar em contato com você para mantê-lo informado, quando necessário, sobre agendamentos dos seus exames, bem como sobre o andamento e os resultados deles e possíveis necessidades de procedimentos confirmatórios ou novas coletas; 3) Colaborar com o desenvolvimento de novos produtos, serviços, eventos e oportunidades promovidas pela **XXX**; 4) Gerar análises e estudos que contribuam com a melhoria de nossas atividades e aperfeiçoem o uso e a experiência interativa em nossos sites, plataformas, produtos e serviços; 5) Transferência de dados para terceiros parceiros da **XXX** que atendam aos requisitos técnicos e para as finalidades presentes em nossa Política de Privacidade; 6) Promover ações de engajamento e disponibilização de programas de monitoramento, dicas e orientações em relação a sua própria saúde; 7) Notificá-lo acerca de nossas campanhas educacionais e de marketing, as quais terão o intuito de auxiliá-lo a melhorar a sua saúde e bem-estar; 8) Permitir contato direto da **XXX** com seu médico e direcionamento precoce de suas informações de saúde e exames para que seu cuidado possa ser realizado de forma ágil e efetiva; 9) Com base nos seus dados de saúde, convidá-lo a participar das iniciativas de prevenção, promoção e atenção à saúde desenvolvidas por parceiros, sem que, desta forma, seus dados sejam compartilhados com estes, que não os profissionais de saúde que venham a prestar atendimento a você; 10) Demais finalidades presentes em nossa Política de Privacidade.

Informamos também que seus dados poderão ser armazenados e utilizados para o atendimento de obrigação legal ou regulatório que a **XXX** tenha que cumprir, bem como para o exercício regular de direitos, conforme expresso na Lei Geral de Proteção de Dados (lei nº 13.709/2018).

Vazamento de Dados

Delegacia de Crimes Cibernéticos vai apurar vazamento de dados sobre menina de 10 anos

Polícia Civil deu detalhes, nesta terça-feira, da prisão do tio que estuprou a criança em São Mateus

ELAINE DAL GOBBO

18/08/2020 14:39 | Atualizado 19/08/2020 18:06

A Delegacia de Crimes Cibernéticos do Estado já foi acionada para apurar o vazamento de informações sobre a menina de 10 anos estuprada pelo tio em São Mateus, norte do Estado, como nome e endereço, postadas nas redes sociais. A informação foi divulgada na tarde desta desta terça-feira (18), em coletiva de imprensa sobre a prisão do tio, de 33 anos, que engravidou a vítima e estava foragido em Minas Gerais.

IPACOM
Instituto Paranaense de Compliance

Vazamento de Dados

CORREIO BRAZILIENSE

PUBLICIDADE

BRASIL

Operadora de plano de saúde diz que ataque hacker vazou dados de clientes

Segundo a Hapvida, as informações potencialmente acessadas incluem dados cadastrais como nome, endereço, CPF e CNPJ de clientes

Vazamento de Dados

HOME / NOTÍCIAS

Pacientes de cirurgia plástica são expostos em vazamento de dados

Os arquivos, armazenados em um banco de dados da Amazon Web Services, continham informações pessoais, fotos sensíveis e documentos

Vinicius Szafran, editado por Cesar Schaeffer 14/02/2020 17h22

Vazamento de Dados

Uma grave brecha de segurança na Gastroclínica Cascavel, um dos principais centros médicos especializados em sistema digestório do estado do Paraná, levou à exposição de dados pessoais de pacientes e médicos, bem como laudos completos de exames. Os arquivos estavam disponíveis livremente e sem nenhum tipo de criptografia ou verificação de credenciais a partir de um link no próprio site da empresa.

Vazamento de Dados

Covid-19

Secretária de Saúde de Três Barras quer investigação por vazamentos de exame e áudio restritos à Saúde

30 Abril 2020 10:05:00

Cópia foi encaminha via WhatsApp para técnicos da secretaria de Saúde de Canoinhas com o objetivo de planejar ações conjuntas

Vazamento da imagem do exame do rapaz que testou positivo para Covid-19 motivou a secretaria de Saúde de Três Barras a registrar, na Delegacia de Polícia do município, boletim de ocorrência (BO) nesta quarta-feira (29).

O compartilhamento da foto através do aplicativo WhatsApp começou no final da tarde de terça-feira, 28.

IPACOM
Instituto Paranaense de Compliance

Referências

- https://lgpdesaude.com.br/wp-content/uploads/2019/08/LGPD_digital_v3-atualizado.pdf
- http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
- http://conteudo.anahp.com.br/cartilha-lgpd-anahp
- https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf

IPACOM
Instituto Paranaense de Compliance

Guia 05
LGPD na Saúde - Aspectos Legais e Regras Específicas Para o Setor

ELABORAÇÃO
Ana Paula Aleixo
Camilla M. Ribas da Silva
Marizete Figueiredo

COORDENAÇÃO
Letícia Sugai