LGPD NA SAÚDE

GIAMBERARDINO
E FÁVERO
ADVOGADOS ASSOCIADOS

I N T R O D U Ç Ã O

A preocupação com a segurança da informação e com os dados pessoais envolve toda a rotina de um profissional da saúde. O tema, aliás, ganhou novos e mais definidos contornos a partir da vigência da Lei Geral de Proteção de Dados, inclusive com a previsão de sanções administrativas em caso de descumprimento das diretrizes nela estabelecidas.

Esse material apresenta conteúdo prático para quem atua na área e gostaria de entender mais sobre a nova legislação.

A Lei n. 13.709, de 14 de agosto de 2018, também conhecida como Lei Geral de Proteção de Dados Pessoais ou LGPD rege o tratamento de dados pessoais realizado por pessoa natural ou por pessoa jurídica de direito público ou privado. Contudo é importante assinalar que, em caráter internacional, as primeiras preocupações sobre o tema remontam à década de 1950, ao passo que as primeiras legislações sobre proteção de dados pessoais datam da década de 1970 e 1980.

A LGPD brasileira foi fortemente influenciada por essas diretivas internacionais e por regramentos da OCDE, buscando, em síntese, proteger o titular dos dados e prever meios de responsabilização quando verificar desvio de finalidade e uso indevido de dado pessoal.

Trata-se de normativa extremamente abrangente, devendo ser adequada aos mais diferentes contextos em que será aplicada. A intenção dessa publicação consiste em apresentar os seus panoramas gerais, e, especialmente, contextualizá-los em forma de respostas e orientações aos profissionais da área de saúde.

LGPD

OS DADOS PESSOAIS PASSARAM A SER PROTEGIDOS NO BRASIL SÓ AGORA?

Na verdade, os dados pessoais já são, há algum tempo, objeto de proteção pela legislação brasileira. Eles integram um conjunto de atributos dos direitos de personalidade, nos quais se incluem uma ampla gama de direitos.

O art. 5°, da Constituição Federal, garante, por exemplo, a inviolabilidade da intimidade e da vida privada. No mesmo sentido ele também protege elementos que são caros aos direitos de personalidade: liberdade de consciência e de crença, livre convicção filosófica e política, inviolabilidade de domicílio, sigilo de correspondência e comunicações, dentre outros.

Além da Constituição Federal, o Brasil já contava com leis que asseguravam questões convergentes com as atuais regras dispostas na LGPD.

É o que ocorre com o Código de Defesa do Consumidor (Lei n. 8.078/1990), com a Lei do Cadastro Positivo (Lei n. 12.414/2011) e com o Marco Civil da Internet (Lei n. 12.965/2014), que estabelecem princípios, garantias, direitos e deveres sobre o tratamento de dados, demonstrando, a todo tempo, especial preocupação com o uso e compartilhamento dessas informações sobre pessoas.

• O QUE É A LGPD?

É a Lei que regulamenta como se deve operar o tratamento de dados pessoais. Entende-se por tratamento de dados pessoais todo o conjunto de operações que abarca a coleta, retenção, alteração, retificação, compartilhamento e exclusão de dados pessoais.

- # QUAL A IMPORTÂNCIA DESSA LEI?

Com a evolução da tecnologia e o avanço de uma sociedade de informação, que é associada com a comercialização de dados com fins econômicos e políticos, cresceu significativamente a preocupação com o tema.

Disso decorre a importância dessa nova Lei, a fim de regulamentar a circulação de dados pessoais, e, com isso, proteger os direitos fundamentais e o livre desenvolvimento da personalidade da pessoa.

Ou seja, a legislação de forma alguma proíbe o tratamento de dados pessoais, pelo contrário. Ela exige fluxos adequados e critérios específicos que, se forem atendidos, permitirão que a atividade seja segura e esteja conforme a regra vigente.

- # QUAL O ÂMBITO DE APLICAÇÃO DA LEI?

Os regramentos estabelecidos pela LGPD se aplicam a qualquer operação realizada ou destinada ao Brasil, inclusive aqueles fluxos estabelecidos no exterior, mas que tenham dados coletados em território brasileiro.

Para fins didáticos consideraremos nessa publicação a expressão dados pessoais ou informações pessoais como sinônimos, ainda que haja distinção técnica entre elas em um nível de detalhamento de governança que não convém aos objetivos desse material.

E QUANDO NÃO SE APLICA A LGPD?

As regras da LGPD não se aplicam apenas em algumas hipóteses. Destacam-se: a) o tratamento de dados realizado para fins exclusivamente particulares; b) para fins jornalísticos, artísticos, acadêmicos; c) para segurança/defesa nacional; d) para atividades de investigação e repressão de infrações penais.

Ainda assim, em que pese não ser aplicável a legislação em sua inteireza, a literatura e jurisprudência mais atualizada sobre o tema compreende como um direito fundamental, de forma que os princípios normativos devem ser aplicados em todas essas hipóteses.

ATENÇÃO: Na área da saúde, a LGPD nunca deve ser desconsiderada, salvo para dados rigorosamente anonimizados ou para cumprimento de requisições do Sistema de Justiça. No que se refere à área acadêmica, que envolve pesquisa com seres humanos, há muito tempo existem diversas regulações exigidas em Comitê de Ética e Pesquisa convergentes com a LGPD e de extremo rigor com o seu tratamento.

- **FUNDAMENTOS DA LGPD**

São fundamentos da Lei Geral de Proteção de Dados Pessoais:

- Respeito à privacidade;

- Respeito à autodeterminação informativa;

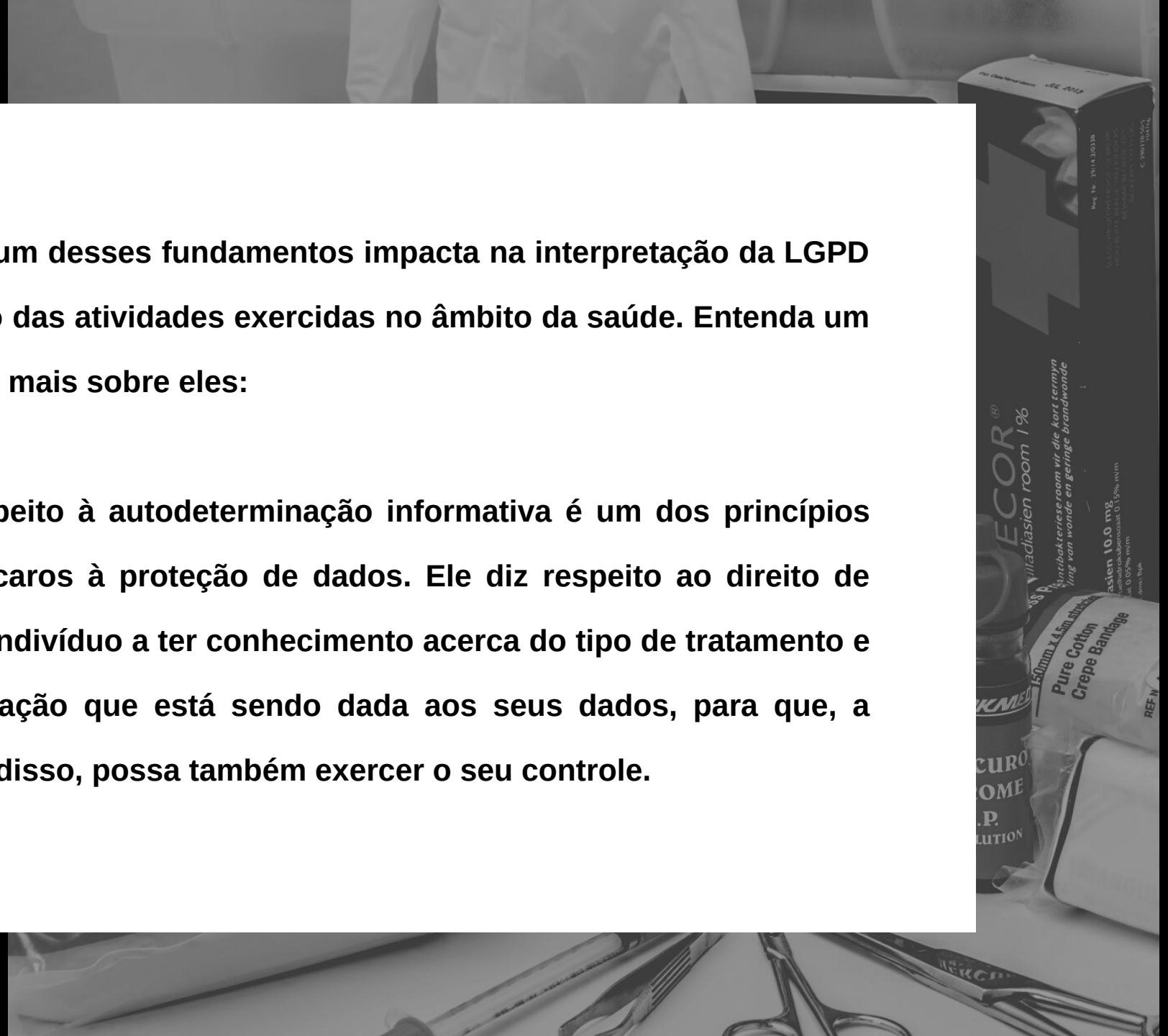
- Liberdade de expressão, de informação, de comunicação e de opinião;

- Inviolabilidade da intimidade, da honra e da imagem;

- Desenvolvimento econômico e tecnológico e a inovação;

- Livre iniciativa, livre concorrência e a defesa do consumidor; e

- Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.



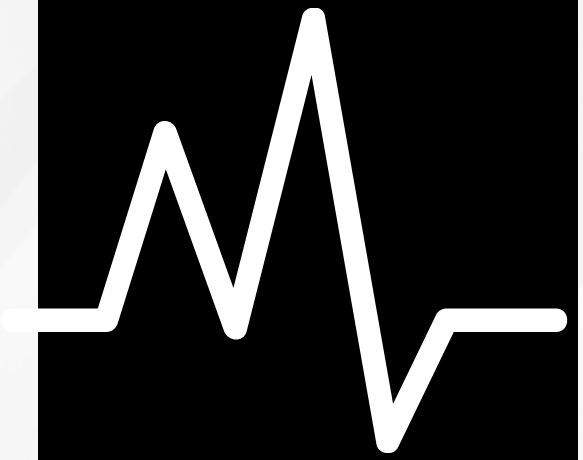
Cada um desses fundamentos impacta na interpretação da LGPD dentro das atividades exercidas no âmbito da saúde. Entenda um pouco mais sobre eles:

O respeito à autodeterminação informativa é um dos princípios mais caros à proteção de dados. Ele diz respeito ao direito de cada indivíduo a ter conhecimento acerca do tipo de tratamento e destinação que está sendo dada aos seus dados, para que, a partir disso, possa também exercer o seu controle.

- **DE ONDE VEM O PRINCÍPIO DA AUTODETERMINAÇÃO INFORMATIVA?**

Com o uso massivo de tecnologias, a proteção de dados pessoais assume função pública de extrema relevância.

A partir da década de 80, iniciou-se a discussão em diversos países sobre a regulamentação da proteção de dados pessoais, o que inclui marcos normativos importantes. A polêmica envolvendo o CENSO populacional por meio do cruzamento de dados foi uma tônica constante em diferentes países, como Suécia, Estados Unidos, Alemanha, Reino Unido.



Não por acaso são esses os países pioneiros em correlacionar tecnologia e monitoramento de dados para políticas públicas, inaugurando as primeiras leis de proteção de dados pessoais.

Em 1983, a Corte Suprema Alemã realiza o julgamento sobre a Lei do Censo. Trata-se de outro importante marco que influencia todo o mundo sobre o conceito de autodeterminação informativa. Em síntese, significa dizer que o maior problema não estava mais no consentimento do indivíduo em fornecer o dado ou de ter uma informação sua revelada de forma indesejada. Tratava-se, antes de tudo, de assegurar mecanismos de controle sobre o fluxo de informações que lhe dissesse respeito.

CONCEITUAÇÕES ESTABELECIDAS PELA LGPD

O principal objeto da legislação é o dado pessoal. A própria legislação tem o cuidado de trazer o conceito de cada categoria que é objeto de proteção legal em diferentes níveis de responsabilidade. São elas:

- **dado pessoal: informação relacionada a pessoa natural identificada ou identificável;**
- **dado pessoal sensível: 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;**
- **dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;**
- **banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.**

- **O QUE SÃO DADOS PESSOAIS E QUAIS SÃO SUAS CATEGORIAS SEGUNDO A LEI?**

Para fins da LGPD, são considerados dados pessoais quaisquer informações relacionadas à pessoa, de forma identificada ou identificável.

A pessoa identificada dispensa maiores conceituações. Tratam-se dos casos em que se reconhece a pessoa a quem se atribui o dado. Exemplo: informações consignadas em cadastro de entrada na portaria, fotografia, biometria, fichas clínicas, exames laboratoriais, imagens captadas em câmeras de segurança, informações veiculadas por email, whatsapp, cadastro de atendimento, dentre outras.

Por sua vez, os dados identificáveis representam todas as hipóteses em, que embora não haja a identificação imediata da(s) pessoa(s), elas podem ser identificadas mediante agregação de outras informações existentes. Exemplo: atendi uma pessoa portadora de neoplasia raríssima; no meu consultório atendo duas crianças ruivas que não conheceram seus pais.

Dentre os dados pessoais, a Lei exige uma categorização e concede especial relevância para proteção aos denominados dados pessoais sensíveis. Trata-se de um complemento – e não uma distinção – sobre as categorias já abordadas de dados pessoais identificados ou identificáveis.

Os dados pessoais sensíveis são considerados como aqueles que remontam a origem racial ou étnica, religião, opinião política, saúde, vida sexual e dado genético ou biométrico.
Tratam-se de dados que devem ser especialmente protegidos, pois têm um maior potencial de discriminação, em especial, se forem utilizados em processos de inteligência artificial.

- **E O QUE NÃO SÃO DADOS PESSOAIS?**

Os dados anonimizados (aqueles cujo titular não possa ser identificado) não se encontram dentro do escopo da LGPD e, como regra geral, afastam a sua aplicação.

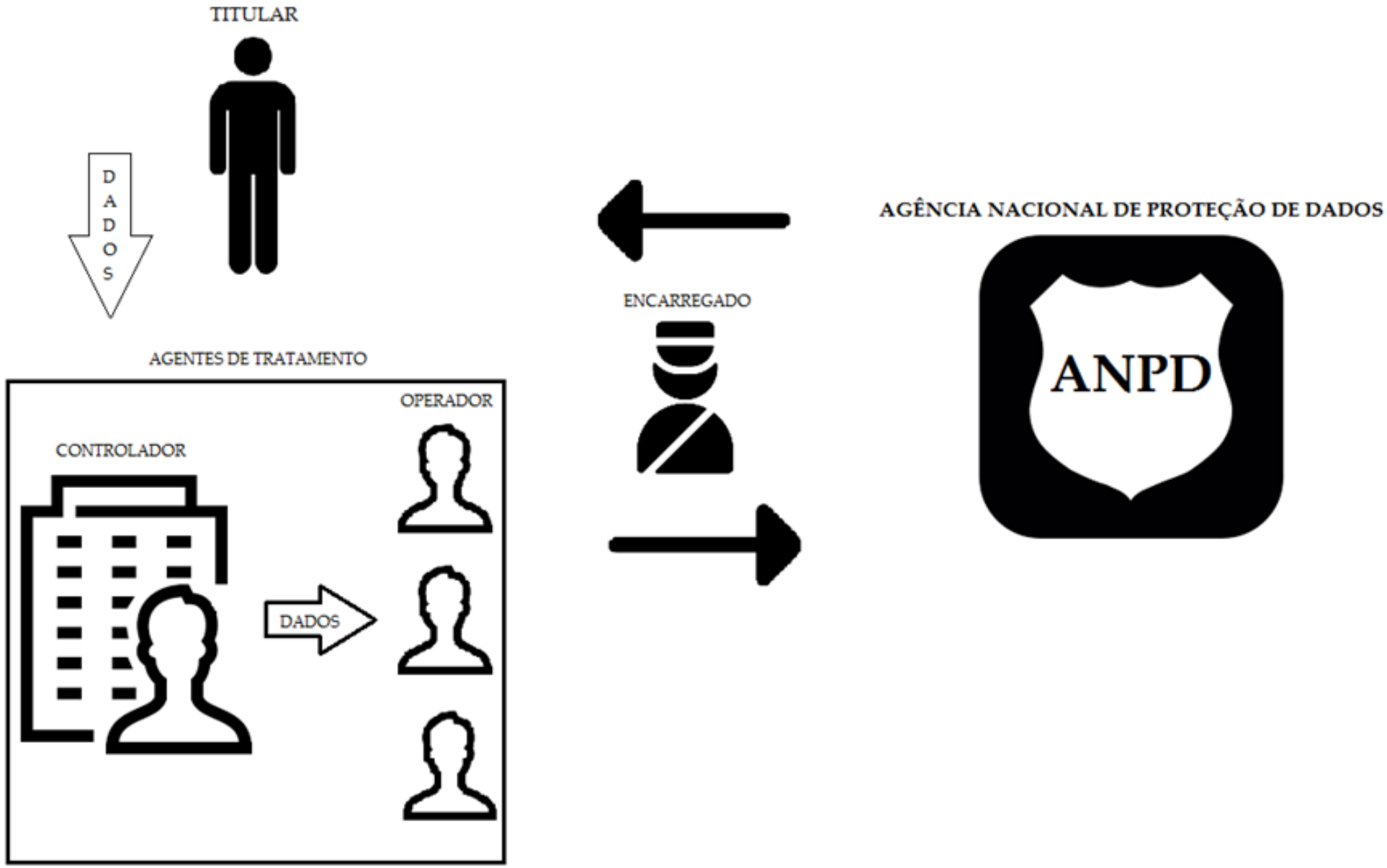
Nesse aspecto reside uma importante diferença já abordada: o dado não identificado e o dado não identificável.

O dado não identificável representa especificamente o dado anonimizado. Ou seja, são aqueles dados em que a pessoa definitivamente não será especificada ou reconhecida.

• SUJEITOS DA LGPD

São os sujeitos da LGPD:

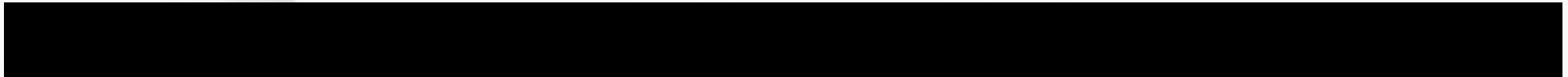
- **Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Pode ser um paciente, um acompanhante, visitante, qualquer pessoa que trabalhe ou preste serviços na instituição, dentre outros.**
- **Controlador: pessoa natural ou jurídica, de direito público ou privado, 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.**
- **Encarregado: 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);**
- **Agentes de tratamento: o controlador e o operador.**


TITULAR
DADOS
AGENTES DE TRATAMENTO
OPERADOR
CONTROLADOR
DADOS
ENCARREGADO
AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS
ANPD

No caso dos Hospitais, Planos de Saúde, clínicas ou instituições congêneres, estes se identificam como "controladores" quando recebem os dados dos pacientes e realizam o seu tratamento. De outro lado, os colaboradores são todos aqueles que trabalham no respectivo local, qualificando-se, neste caso, como "operadores" do dado. Eles atuam em nome do controlador e sob a responsabilidade dele.

A eles também se equiparam eventuais serviços terceirizados. Cita-se, como exemplo, os sistemas de informática que são contratados para municiar os trabalhos internos dos profissionais de saúde, como também outros serviços com menor nível de acesso às informações como empresas que emitem boletos bancários, operadoras de cartão de crédito, dentre outros.

Por fim, o "encarregado" é a 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).



- **SAIBA MAIS SOBRE O ENCARREGADO**

O encarregado será o canal de contato junto a categoria profissional e a Autoridade Nacional, sendo o responsável por:

- aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

- receber comunicações da autoridade nacional e adotar providências;

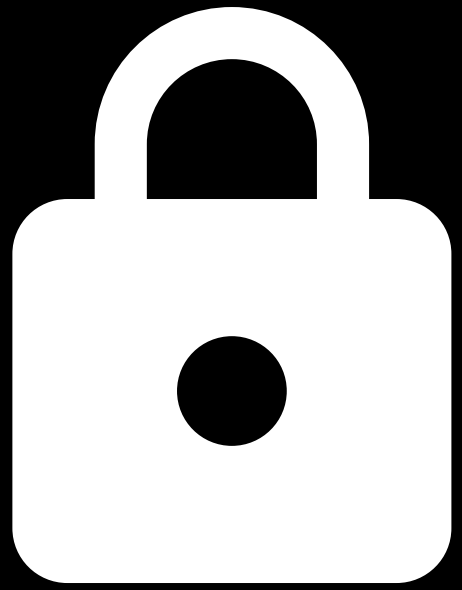
- orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

- executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

O encarregado pode ser pessoa física ou jurídica, inclusive mediante empresas especializadas, não havendo óbice legal que exerça a função em mais de um local. Recomenda-se, nesse sentido, que todos os setores resguardem um contato de e-mail em local visível para denúncias, sugestões e reclamações.

Obs.: A LGPD determina que a identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador. Conforme a proporção do trabalho prestado, os regramentos a serem realizados pela ANPD poderá dispensar a figura do encarregado.

Atualmente discute-se a dispensa para as microempresas e empresas de pequeno porte, mas ainda não há regra específica sobre a matéria, de modo que todos os segmentos estão obrigados pela lei a se regularizarem se ainda não tiverem feito. Até o momento houve apenas orientações sobre o limite de responsabilidade do encarregado.



ANPD: A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão responsável por zelar pela proteção dos dados pessoais, com atividades de fiscalização, regulamentação, promoção e estímulo.

Dentre as suas atribuições, a ANPD poderá:

- estabelecer normas complementares sobre a forma adequada de dar publicidade aos atos de tratamento de dados, o que deverá ser observado pelos agentes de tratamento;

- solicitar a publicação de relatórios de impacto à proteção de dados pessoais;

- solicitar informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado;

- emitir parecer técnico complementar para garantir o cumprimento da LGPD;

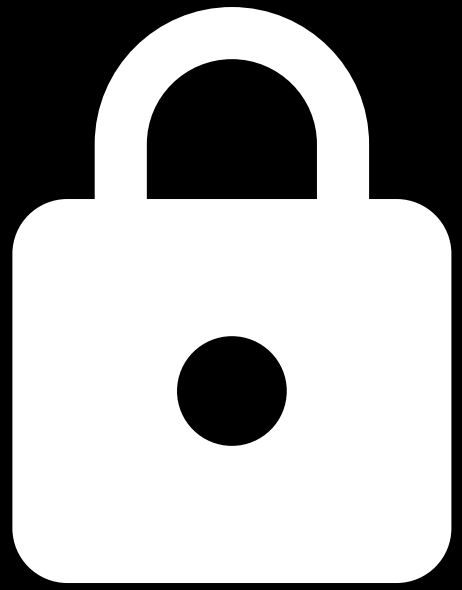
- sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais;

- enviar informe com medidas cabíveis para fazer cessar a violação no tratamento de dados pessoais.

Nesse sentido, a ANPD certamente expedirá diversas normas técnicas complementares e específicas para diferentes atividades, que compreendem ampla gama de serviços.

Cabe, pois, a todos os profissionais ficarem atentos a novas diretrizes sobre o tema.

Além dela, os conselhos profissionais e os responsáveis pela fiscalização de atividades reguladas, como é o caso da Medicina, Enfermagem, Psicologia, Fisioterapia, dentre outros, podem orientar e suplementar regras na qualidade de dever de conduta profissional.



CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE - CRIADO COM A INCUMBÊNCIA DE PRESTAR ASSESSORAMENTO TÉCNICO DA ANPD, COM MEMBROS DE ÓRGÃOS PÚBLICOS, ENTIDADES PRIVADAS E REPRESENTANTES DA SOCIEDADE CIVIL.

- **RESPONSABILIDADE DO CONTROLADOR E DO OPERADOR**

O controlador e o operador respondem solidariamente pelos danos causados pelo tratamento dos dados que lhes foram confiados. Os agentes de tratamento só não serão responsabilizadas quando provarem uma das hipóteses:

- que não realizaram o tratamento de dados pessoais que lhes é atribuído;

- que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

- que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Nesse sentido que a delimitação de rotinas, fluxos de compartilhamento de dados e instrumentos que vinculem as obrigações da instituição com regras de conduta para a sua rede de colaboradores - internos ou externos – garante a mitigação de riscos da sua atividade.

Mais do que isso, embora não evite a sua responsabilização solidária, caso o empregado haja incorrido em alguma infração das regras internas, pode sujeitá-lo às penalidades previstas na legislação trabalhista, e, conforme o caso, o direito de regresso pelos valores pagos em razão de sua falta.

REGRAMENTOS SUPLEMENTARES À LGPD NA ÁREA DE SAÚDE

CFM - CONSELHO FEDERAL DE MEDICINA

O Conselho Federal de Medicina disciplinou a política de privacidade dos dados sobre o uso do Whatsapp no âmbito da saúde, tendo como especial escopo a proteção de dados pessoais. Nessa Resolução está previsto como os Conselhos Profissionais devem tratar os dados pessoais e as diretrizes de sua política.

Como órgão regulatório de importante profissão no âmbito da saúde, destaca-se o Código de Ética Médica (Res. CFM n. 2.217/2018) que prevê recursos como o consentimento do paciente para compartilhamento de informações, sigilo profissional, manuseio de documentos e pesquisa médica.

Posteriormente, também foram editados atos específicos voltados a orientar o uso de Whatsapp e a relação da conduta profissional médica diante de recursos tecnológicos. Confira abaixo os seus principais fundamentos:

- o uso de novas tecnologias consiste em medida irreversível e que traz incontáveis benefícios ao melhor diagnóstico e posterior prognóstico dos pacientes;

- os grupos de Whatsapp devem ser formados entre médicos e pacientes, ou então, exclusivamente por profissionais médicos para discussão de casos que demandem a intervenção de diferentes especialidades;

- a veiculação desses dados não desnatura o dever de sigilo, razão pela qual consiste em violação de dever funcional a abertura dessas discussões para profissionais não médicos ou para profissionais sem relação com o tratamento;

- a veiculação desses dados não afasta o artigo 75 do Código de Ética Médica, ou seja, não devem fazer referência a casos identificáveis, exibir pacientes ou seus retratos em anúncios, tampouco em meio de comunicação em geral (inclusive quando houver autorização do paciente!);

- cada participante do grupo de Whatsapp é pessoalmente responsáveis pelas informações, opiniões, palavras e mídias disponibilizadas.

- **OUTROS CUIDADOS NOS PRONTUÁRIOS MÉDICOS E FICHAS MÉDICAS**

A definição de prontuários e fichas médicas foi objeto de específica proteção na LGPD. Além disso, as normativas sobre prontuários e fichas médicas é regulada de forma específica pela Resolução CFM n. 1.638/2002.

O prontuário médico e as fichas médicas envolvem o conjunto de dados pessoais do paciente e possibilita a comunicação entre membros da equipe multiprofissional mediante o sigilo e o dever ético de cuidado compartilhado entre as especialidades.

Confira abaixo algumas normativas importantes sobre o tema no CFM:

- **A Resolução CFM n. 1.605/2000 trata da necessidade de consentimento para compartilhamento de informação do prontuário e ficha médica;**
- **A Resolução CFM n. 1.821/2007 (com alterações posteriores) trata sobre uso de sistemas digitalizados de prontuários médicos;**
- **A Resolução CFM n. 1.819/2017 proíbe a colocação do diagnóstico codificado (CIF) ou tempo de doença no preenchimento das guias para as operadoras de saúde, a fim de evitar que dados sensíveis sejam triados com fins discriminatórios.**
- **OBS. A proibição de veiculação da CID também foi reconhecida em decisões do Tribunal Superior do Trabalho (TST), sendo vedada a obrigatoriedade de inclusão do código CID nos atestados médicos dos trabalhadores.**

- **ANS**

A Agência Nacional de Saúde também lançou Código de Boas Práticas e a Nota Técnica n. 03/2019, que implementa requisitos da LGPD na ANS. Também foi criado o Comitê de Padronização das Informações em Saúde Suplementar – COPISS, que estabeleceu padrão obrigatório para Troca de Informações na Saúde Suplementar – TISS, por meio da Resolução Normativa n. 305.

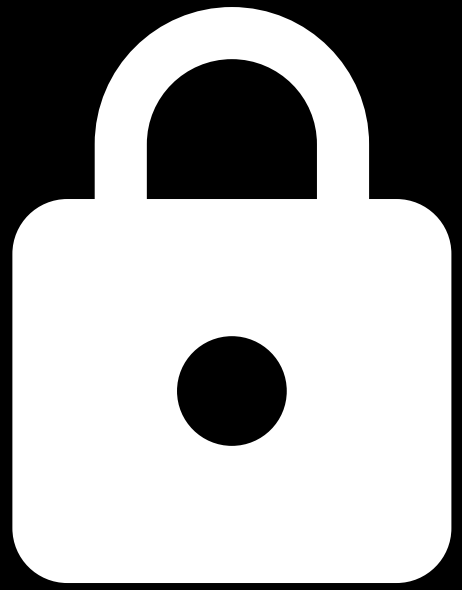
Isso regulamenta a coleta e compartilhamento entre prestadoras de saúde e operadoras de plano de saúde, atendendo ao conceito legal de cumprimento de obrigação regulatória.

A ANS também garante segurança jurídica por meio de Resoluções Normativas já antigas, como é o caso da RN n. 255/2011 e RN n. 389/2015, que versam sobre os responsáveis e os fluxos de informações relativas à assistência à saúde.

- **ANVISA**

A ANVISA exerce a importante função de normatizar, controlar e fiscalizar produtos, substâncias e serviços de interesse para saúde (art. 2º, inciso III, da Lei n. 9.782/1999). Disso decorrem a edição de Resoluções como a RDC n. 09/2015 e 10/2015, que é importante na área de pesquisa e de produção de fármacos.

Ela também editou o Guia n. 38/2020 – Princípios e práticas de cibersegurança em dispositivos médicos. Nessa publicação constam as melhores práticas sobre procedimentos, rotinas e métodos adequados ao cumprimento dos requisitos exigidos pela agência.



DICAS DE PROTOCOLOS SOBRE SEGURANÇA DA INFORMAÇÃO NA ÁREA DE SAÚDE

Se você deseja instituir um protocolo de segurança da informação. lembre de algumas questões importantes:

- O uso de aparelho pessoal no ambiente de trabalho impede o controle sobre regras importantes de segurança: qual a forma de backup que cada um faz do seu aparelho celular ou tablete/laptop; para quem o colaborador empresta o aparelho; quais aplicativos fez download ou utiliza; em quais canais ele navega. Isso significa que qualquer clonagem, perda, roubo ou extravio desse aparelho poderá ter repercussões para o seu ambiente de trabalho. Portanto, prefira, sempre que possível, usar meios institucionais de comunicação;

- Os e-mails utilizados e os canais de comunicação adotados devem ser criptografados. Apesar de parecer uma regra elementar há muitos serviços prestados no mercado sem essa característica.

- A rede de internet e de fluxo de informações internas deve ser restrita ao ambiente de trabalho. Por isso evite utilizar redes de internet públicas, sejam elas sem senha ou compartilhadas com visitantes. São recursos fáceis e baratos de serem adaptados que mitigam muitos riscos.

- **TERMOS DE CONFIDENCIALIDADE**

Além de estabelecer um fluxo de dados de acordo com o ato praticado e adotar todas as políticas de segurança da informação, é aconselhável, também, ajustar os contratos perante os colaboradores internos e externos, de modo a contemplar termos de confidencialidade.

Os serviços terceirizados que tenham acesso a dados pessoais também devem ter ciência de que as informações veiculadas em razão do contrato de prestação de serviços se submetem aos regramentos da LGPD, não podendo, de qualquer forma, compartilhar, repassar ou desvirtuar a finalidade das informações recebidas.

- **ATENÇÃO - Na execução de suas funções, o agente de tratamento de dados pessoais deve sempre ter em mente:**

- a FINALIDADE pela qual aqueles dados lhe foram confiados, de forma que sejam tratados os dados adequados e necessários para alcançar o motivo da sua coleta;

- a TRANSPARÊNCIA no tratamento dos dados que lhe foram confiados, de modo que a Instituição possa prestar contas ao titular sobre como seus dados estão sendo utilizados e armazenados, garantindo, também, o livre acesso, a fim até mesmo de garantir eventuais retificações e, consequentemente, manter a qualidade dos dados;

- a SEGURANÇA nos trâmites internos, prevenindo-se eventual divulgação indevida e malversação dos dados.

Os três eixos ora relacionados compreendem o conjunto de práticas que visam garantir a confidencialidade, integridade e disponibilidade de dados aos interessados por qualquer banco de dados estruturado. Explica-se:

- Confidencialidade: é a restrição de acesso a dados pessoais exclusivamente àqueles que tenham legitimidade para o seu acesso, seja em razão do seu trabalho ou do direito conferido ou não vedado por lei.

- Integridade: garantia de que os dados serão mantidos nas mesmas condições na qual foram coletados, ou seja, que não serão desvirtuados ou alterados.

- Disponibilidade: garantia de que os dados estarão disponíveis mediante solicitação de pessoa legitimada a ter acesso.

Uma vez observados esses pressupostos, por meio de práticas consubstanciadas em processos internos e externos, treinamentos de equipe e políticas de segurança da informação, estarão sendo respeitados os conceitos chave para uma governança de dados pessoais.

- **DIREITOS DO USUÁRIO**

Garante-se que o usuário possa saber quais são os dados existentes em cada banco de dados, como também possa corrigir, completar, anonimizar, bloquear ou eliminar os dados de forma integral ou parcial, desde que isso não afete regras legais ou regulatórias sobre a saúde.

Significa dizer que nem todo pedido realizado pelo titular deve ser aceito. Antes de tudo é necessário analisar as regras existentes sobre o tema e ponderar sobre o grau de alcance de cada direito.

Certamente, no caso da saúde, há o direito de acesso pelo titular ou por pessoa legitimada a esse fim, mas não há o direito de pedir a eliminação ou exclusão de todos os dados que devam ser armazenados no âmbito da instituição como, por exemplo, os prontuários médicos.

A legislação também assegura a portabilidade dos dados e a informação das entidades públicas e privadas com as quais houve o compartilhamento dos seus dados. Para tanto devem ser adotados mecanismos que registrem as hipóteses e as características desses compartilhamentos.

Com a finalidade de elucidar os principais aspectos já tratados, que dizem respeito aos direitos dos titulares de dados pessoais com os seus respectivos princípios disciplinados na LGPD, correlaciona-se na tabela abaixo:

Direitos do titular do dado pessoal	Princípio correlacionado
Acesso aos dados pessoais informados ou compartilhados	Princípio do livre acesso, transparência, responsabilização e prestação de contas
Limitação de compartilhamento	Princípio da finalidade, adequação e necessidade
Dados fidedignos e preservados	Princípio da qualidade dos dados, segurança, prevenção, não discriminação

Também existem hipóteses onde os Hospitais e instituições de saúde, de modo geral, podem tratar o dado independentemente do consentimento do titular. É o caso das hipóteses de emergência ou quando imperar o melhor interesse da criança ou do adolescente.

Nesse contexto que se afirma que a finalidade do dado está respeitada dentro do contexto em que ele é tratado. Ou seja, uma vez sendo atendido dentro do ambiente hospitalar, a instituição se encontra legitimada a praticar atos voltados ao bem estar do paciente, de forma que tudo aquilo que não seja desvirtuado desse contexto encontra-se resguardado pelo legítimo interesse da instituição.

Todavia, os direitos do paciente e a sua autodeterminação informativa também são princípios caros ao setor de saúde. Por isso, apesar da previsão de urgência e emergência, não se afasta os deveres éticos do profissional de saúde quanto ao direito do consentimento livre e esclarecido, mediante regramentos já há muito tempo adotados.

- **TERMO DE CONSENTIMENTO**

Conforme já mencionado, em algumas hipóteses é exigido o consentimento do titular dos dados ou de seu responsável legal para o tratamento de dados.

Como direito do paciente também é necessário que ele e/ou seu responsável legal estejam cientes de que os dados serão tratados. É claro que a busca por um serviço de saúde pressupõe essa concordância, mas há limites que nem sempre são evidentes.

Por esse motivo consignamos algumas orientações sobre a coleta do Termo de Consentimento:

- deve ser fornecido por escrito ou por outro meio que demonstre a sua manifestação de vontade;

- deve constar em cláusula destacada incluindo a sua finalidade;

- se houver compartilhamento mediante aplicativos de celular, acesso por internet, incluindo-se o compartilhamento com profissionais ou instituições de saúde não pressupostas no atendimento, recomenda-se a coleta de consentimento específico e orientações por escrito sobre a política adotada pela instituição;

- deve referir-se a finalidades determinadas (autorizações genéricas ou com conteúdo enganoso ou abusivo serão consideradas nulas);

- pode ser revogado a qualquer momento pelo titular.

Obs.: se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade podendo o titular revogar o consentimento. Recomenda-se tratativas por escrito, a fim de comprovar o consentimento do usuário.

- **TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES**

A LGPD também dispensa especial preocupação à proteção dos dados de crianças e adolescente. Em qualquer hipótese, o tratamento do respectivo dado deve atender o seu melhor interesse.

Dentre os requisitos específicos exigidos pela lei, o tratamento de dados de crianças e adolescentes, quando não decorrer de norma legal, deve ser realizado com consentimento específico de - ao menos - um dos pais ou responsável.

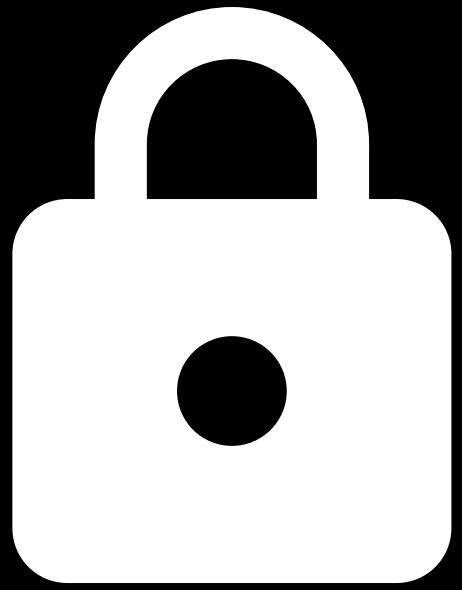
Tal regra é excetuada na hipótese de não ser possível contatar os pais ou o responsável legal. Neste caso, autoriza-se a realização do tratamento de dados, mas em nenhum caso poderá ser repassado a terceiros que não sejam vinculados à rotina institucional e ao contexto da coleta.

O tratamento deve atender ao MELHOR INTERESSE do titular, e deve ser precedido de consentimento de ao menos um responsável legal. O consentimento é excetuado apenas em duas hipóteses, vedado o repasse a terceiros:

- para contatar os pais, devendo o dado ser utilizado somente para isso, sem armazenamento;

- para proteção da criança/adolescente.

Aplicam-se, ainda, as exceções às hipóteses de consentimento já exaradas em tópico específico, como, por exemplo, tratar-se de situações de emergência ou de cumprimento de ordem legal ou judicial.

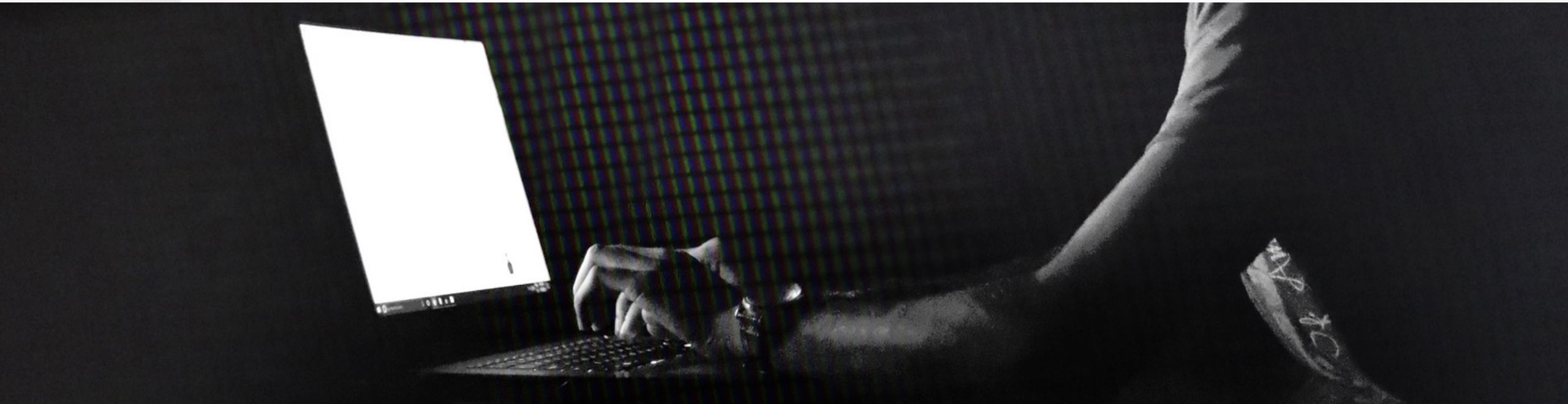


FLUXO DE DADOS

Conhecer o exato fluxo transcorrido pelo dado é vital não apenas para a mitigação das responsabilidades, mas também para que a instituição possa demonstrar a adequada fiscalização a esse respeito. Deve-se, portanto, mapear toda atividade praticada, e, a partir daí, verificar o caminho percorrido pelo dado. Para tanto são adotadas as seguintes providências:

1. **Categorizar a atividade realizada;**
2. **Verificar os dados estritamente necessários para o fim específico, e categorizá-los (se sensíveis ou não; se de criança e adolescente ou não);**
3. **Identificar a porta de entrada do dado;**
4. **Identificar os atos de tratamento operacionalizados na instituição;**
5. **Documentar se houve qualquer tipo de transferência/compartilhamento dos dados;**
6. **Documentar o armazenamento do dado;**
7. **Documentar o descarte do dado, se for o caso.**

A sedimentação de um fluxo para cada atividade deve servir, também, para a consolidação dos respectivos procedimentos internos, de modo a especializar cada operador e aperfeiçoar não apenas o adequado tratamento dos dados, mas também estratégias para a otimização dos recursos materiais e humanos.



- **CONSERVAÇÃO DE DADOS PESSOAIS**

Segundo a LGPD, a regra é que os dados sejam eliminados após o alcance da finalidade pela qual foram informados, sendo que a conservação é possível apenas nas seguintes hipóteses:

- cumprimento de obrigação legal ou regulatória pelo controlador;

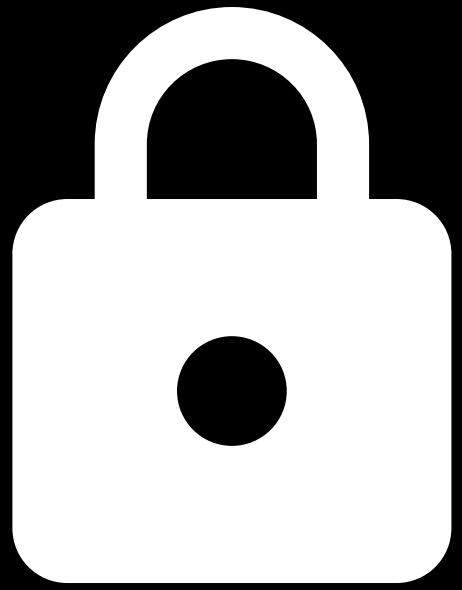
- estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

- transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

- uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

No caso da área de saúde é justificável a preservação do dado pelo cumprimento de obrigação legal ou regulatória.

No entanto, o armazenamento, como atividade que também caracteriza o “tratamento de dados”, continua a obedecer aos princípios e regras estabelecidos na legislação, o que deve ser objeto de análise e discussões periódicas em cada ambiente da instituição sobre a política adotada.



COMUNICAÇÃO DE INCIDENTE À ANPD

Conforme a LGPD, o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Em que pese ainda inexistir qualquer normatização acerca dessa matéria, o Relatório produzido dentro de uma política de controle de incidentes de segurança municia os requisitos legais e previne responsabilidades.

- **PENALIDADES**

Administrativamente, podem ser aplicadas as penas de:

- advertência;

- multa de até 2% (dois por cento) do faturamento;

- publicização da infração;

- bloqueio e eliminação dos dados pessoais.

- suspensão parcial do funcionamento do banco de dados a que se refere à 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 à 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 penalidades entraram em vigor a partir do ano de 2021.

Obs.: As penas administrativas não excluem eventuais responsabilizações civis, penais, e de improbidade administrativa.

- **O QUE ATENUA A PENALIDADE?**

A penalidade será atenuada se for verificada:

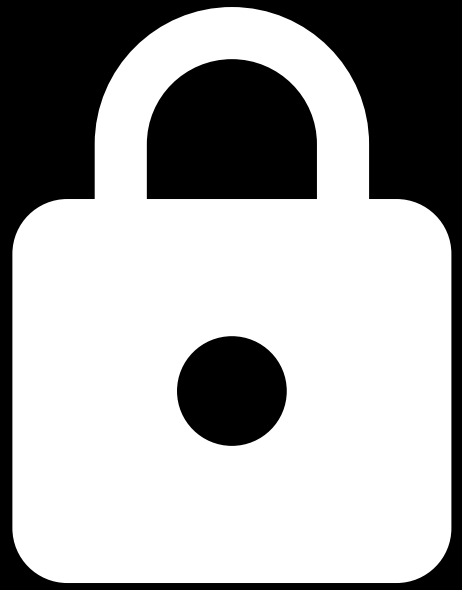
- a primariedade da infração;

- se o local comprovar que diligenciou medidas de mitigação de riscos e preocupou-se com a LGPD;

- se o local comprovar que adota boas práticas sobre LGPD.

Nesse sentido, a documentação sobre as providências adotadas para regularização da atividade à luz da LGPD, incluindo-se a contratação de assessoria, a distribuição e fixação de orientações no ambiente interno, bem como o contínuo treinamento dos colaboradores são exemplos de atos tendentes a mitigar a possibilidade de responsabilização.

Isso também auxilia na defesa da instituição caso seja autuada pela ANPD.



ORIENTAÇÕES GERAIS

- A LGPD é aplicável aos hospitais e clínicas de saúde;

- A aplicação da LGPD decorre do cumprimento de normas legais e regulamentares, de modo que certas vezes independem do consentimento do titular de dado pessoal;

- O tratamento dos dados deve ocorrer no mesmo contexto e finalidade da sua coleta (p. ex. prestação de serviços à saúde);

- É recomendável a verificação dos procedimentos internos sobre o fluxo de dados e o contínuo treinamento da equipe, a fim de consolidar uma cultura de proteção de dados pessoais;

- Recomenda-se a adoção de regras por escrito e cartazes orientativos periódicos sobre os direitos e deveres aplicáveis de acordo com a LGPD;

- Recomenda-se a utilização de canais para comunicação interna institucionais como email, telefone institucional, dentre outros, evitando-se uso de aparelhos pessoais;

- Recomenda-se que sejam especificadas atribuições e níveis de acessos nos sistemas informatizados, preferencialmente por meio de senhas, a fim de salvaguardar o acesso estritamente necessário e minimizar riscos de má utilização dos dados coletados;

- Os Hospitais, Laboratórios e clínicas se qualificam como controladores, que são responsáveis pelo tratamento de dados;

- Os controladores devem indicar um encarregado, que será o responsável pela interlocução entre usuários, a instituição e a autoridade nacional de proteção de dados;

- Há possibilidade de compartilhamento de dados com entidades públicas e privadas, desde que resguardadas as orientações e os princípios da LGPD;

- Recomenda-se o monitoramento dos contratos com serviços terceirizados, incluindo-se, preferencialmente, Termo de Confidencialidade e controle dos dados compartilhados;

- Recomenda-se também a periódica verificação dos padrões de segurança dos sistemas informatizados contratados, como também que os colaboradores e empresas se comprometam com uma Política de Proteção de Dados Pessoais;

- Os fluxos internos e as práticas consolidadas consistem em boas práticas, que devem ser veiculadas, por tratar-se de experiência passível de ser adotada em outros locais, além de ser incentivada pela legislação inclusive como atenuante de eventual responsabilização;

- Na hipótese de incidente de segurança deve-se avisar prontamente o encarregado para que avalie a dimensão e adote as providências legais cabíveis.

Clique aqui para preencher o formulário de orçamento