Código de Boas Práticas do Setor da Saúde

FÓRUM PERMANENTE DO SETOR DE SAÚDE
EM PROTEÇÃO DE DADOS E PRIVACIDADE
2026

FenaSaúde
anahp
CMB
CNSaúde
sinog
abramge
FBH
abraidi
Abramed
APOIO: Instituto Consenso

Código de Boas Práticas do Setor da Saúde

FÓRUM PERMANENTE DO SETOR DE SAÚDE
EM PROTEÇÃO DE DADOS E PRIVACIDADE

2026

APRESENTAÇÃO DAS COORDENADORAS

A Lei Geral de Proteção de Dados Pessoais (LGPD) foi sancionada em 2018 e entrou em vigor de forma gradual. Em 2020, a maior parte de seus dispositivos passou a produzir efeitos e foi nomeado o primeiro Conselho Diretor da Autoridade Nacional de Proteção de Dados. Em 2021, teve início a aplicação dos dispositivos relativos às sanções administrativas. Em 2022, a ANPD foi transformada em autarquia de natureza especial e, em 2025, foi editada a medida provisória que iniciou sua transformação em agência reguladora, processo posteriormente consolidado em 2026.

Essa trajetória revela que o regime brasileiro de proteção de dados não deve ser compreendido apenas como um marco legislativo pontual, mas como um sistema jurídico em consolidação. Esse processo não depende apenas da atuação da ANPD, mas também da capacidade dos setores regulados de interpretar a lei à luz de suas especificidades e construir parâmetros próprios de conformidade.

Esse processo é particularmente importante porque a própria LGPD reconhece que a conformidade não se esgota no cumprimento de parâmetros expressamente apontados na lei. O art. 50 confere papel central às regras de boas práticas e de governança, permitindo que os agentes de tratamento formulem parâmetros sobre organização, regime de funcionamento, procedimentos internos, atendimento a titulares, normas de segurança, padrões técnicos, ações educativas, mecanismos de supervisão e medidas de mitigação de riscos. Trata-se de uma previsão especialmente relevante para setores complexos, como o da saúde, em que a aplicação da lei exige a tradução de princípios gerais em orientações concretas, proporcionais e aderentes à realidade operacional dos diferentes agentes.

Nesse sentido, o art. 50 fortalece os mecanismos de autorregulação e reforça a importância de se observar as especificidades setoriais. Ele permite que os próprios setores, a partir de sua experiência técnica, institucional e operacional, contribuam para a construção de parâmetros de conformidade mais claros, efetivos e verificáveis. É justamente nesse espaço de governança colaborativa, responsabilidade setorial e amadurecimento regulatório que se insere o presente Código de Boas Práticas.

No setor de saúde, o tratamento de dados pessoais está diretamente relacionado à própria organização, continuidade e qualidade dos serviços prestados. Dados de pacientes, beneficiários, profissionais de saúde e demais atores da cadeia são utilizados em atividades assistenciais, administrativas, regulatórias, financeiras, científicas e tecnológicas. Essa realidade torna insuficiente uma abordagem meramente formal de conformidade. A aplicação adequada da LGPD exige compreensão das práticas concretas do setor, dos fluxos informacionais existentes, das responsabilidades de cada agente e dos riscos associados a cada contexto de tratamento.

Esse movimento de compreensão das especificidades do setor teve início com o Código de Boas Práticas de Proteção de Dados para Prestadores Privados de Saúde, lançado em 2021 sob coordenação da Confederação Nacional de Saúde, Hospitais, Estabelecimentos e Serviços. A partir daquela experiência, tornou-se evidente a necessidade de ampliar o debate para contemplar outros atores essenciais da cadeia da saúde, cujas atividades são interdependentes e frequentemente envolvem fluxos compartilhados de dados pessoais.

O presente Código nasce, portanto, de um esforço coletivo de atualização, aprofundamento e integração setorial. Ele reúne três segmentos fundamentais: prestadores de serviços de saúde, operadoras de planos de saúde e fornecedores e distribuidores de produtos para a saúde. Embora cada um desses grupos possua características próprias, todos participam de um mesmo ciclo de vida dos dados pessoais no setor.

Na prática, os dados pessoais podem ser tratados em múltiplos contextos. Eles aparecem no atendimento médico presencial ou remoto, no uso de exames e informações clínicas para diagnóstico e tratamento, na emissão de laudos, na gestão de prontuários, na autorização de procedimentos, no faturamento, na auditoria médica, na análise atuarial, na prevenção a fraudes, na rastreabilidade de dispositivos médicos, na interação com profissionais de saúde, no cumprimento de normas da ANS, da Anvisa e de outras autoridades competentes, bem como no desenvolvimento de soluções tecnológicas, pesquisas, programas de suporte ao paciente e iniciativas de melhoria da qualidade assistencial.

Esses exemplos não esgotam a diversidade de operações de tratamento existentes no setor. Ao contrário, servem para evidenciar que a proteção de dados na saúde exige olhar sistêmico. A amplitude desses tratamentos também revela a importância dos dados para a própria continuidade e evolução dos serviços de saúde. Informações pessoais e, muitas vezes, dados sensíveis são indispensáveis para atividades básicas, como identificação do paciente, agendamento, faturamento, cobrança, emissão de documentos fiscais, manutenção de prontuários e cumprimento de obrigações regulatórias. Ao mesmo tempo, são essenciais para iniciativas mais sofisticadas, como telessaúde, monitoramento remoto, gestão de saúde populacional, pesquisa clínica, desenvolvimento de novas tecnologias, uso de inteligência artificial, melhoria de dispositivos médicos e aprimoramento da experiência do paciente.

O desafio, portanto, não está em opor proteção de dados e inovação, mas em criar as condições para que ambas se reforcem mutuamente. No setor de saúde, boas práticas de proteção de dados contribuem para ampliar a confiança, qualificar os serviços prestados e fortalecer as relações com pacientes, beneficiários, profissionais de saúde, parceiros comerciais, autoridades regulatórias e a sociedade.

Foi com essa perspectiva que coordenamos este trabalho. O Código apresenta, em primeiro lugar, uma parte geral dedicada à aplicação da LGPD ao setor de saúde, abordando conceitos essenciais, princípios, bases legais e condições de legitimidade para o tratamento de dados pessoais. Em seguida, avança para diretrizes práticas voltadas às especificidades do setor, tratando de temas que demandam atenção especial, como prontuário eletrônico, telessaúde, relação com terceiros, prevenção e promoção da saúde, auditorias, ferramentas de identificação, atendimento aos direitos dos titulares, relatórios de impacto, segurança da informação e inovação.

Destaca-se que essa nova versão amplia o tratamento dedicado à inovação, incorporando de forma específica os desafios decorrentes do uso da inteligência artificial e de outras tecnologias emergentes no setor de saúde. O Código busca oferecer parâmetros para uma adoção responsável dessas tecnologias, fundada em transparência, governança, supervisão humana, avaliação de riscos e respeito aos direitos dos titulares.

Assim, além de garantir a conformidade dos agentes com a LGPD, este Código tem como objetivo servir como ferramenta de orientação, diálogo e amadurecimento institucional. Seu objetivo é oferecer parâmetros práticos para que os diferentes agentes do setor possam implementar programas de governança proporcionais aos seus riscos, ao seu porte, às suas atividades e ao papel que desempenham na cadeia da saúde.

A tecnologia é um dos pilares do desenvolvimento do setor de saúde, sendo de suma importância para o incentivo à inovação e a produção de conhecimento. A estruturação de programas de governança que sejam ao mesmo tempo robustos e adaptáveis às especificidades do setor é fundamental para incentivar práticas inovadoras que concretizem o direito à saúde no país.

Laura Schertel Mendes

Mônica Fujimoto

SUMÁRIO

PARTE I

LGPD APLICADA

1. INTRODUÇÃO

Este Código de Boas Práticas para o Setor de Saúde é resultado do trabalho desenvolvido no âmbito do Fórum Permanente do Setor de Saúde em Proteção de Dados e Privacidade, que reúne representantes das principais categorias do setor: Prestadores de Serviço de Saúde, Operadoras de Planos de Saúde e Fornecedores e Distribuidores de Produtos para Saúde.

Em 2021 foi lançado o primeiro Código de Boas Práticas de Proteção de Dados para Prestadores Privados de Saúde, coordenado pela Confederação Nacional de Saúde, Hospitais, Estabelecimentos e Serviços (CNSaúde). Na esteira desse Código ficou clara a necessidade de realizar um debate mais amplo que incluísse outros segmentos do setor de saúde, como operadoras de planos de saúde e fornecedores e distribuidores de produtos de saúde.

Com a participação das prestadoras de serviços de saúde, operadoras de planos de saúde e dos fornecedores de produtos de saúde, este guia consolida as melhores práticas de tratamento de dados pessoais no Brasil. Além disso, o amadurecimento da atuação da Autoridade Nacional de Proteção de Dados (ANPD) e, principalmente de suas atividades fiscalizatórias e sancionatórias evidencia a necessidade de uma abordagem proativa do setor, de modo a demonstrar o seu compromisso com a proteção de dados.

Vale destacar que os benefícios da implementação de programas de compliance eficazes não se limitam apenas à proteção dos dados dos titulares. Segundo o Data Privacy Benchmark Study 2023, divulgado pela Cisco, o valor estimado em dólares dos benefícios gerados por programas de privacidade aumentou significativamente em 2023, com ganhos notáveis para instituições de todos os tamanhos. O estudo também ressalta a importância de manter investimentos contínuos em privacidade e segurança da informação, com ênfase na transparência necessária para garantir que os clientes entendam as medidas adotadas pelas instituições.

No mínimo: redução de preço, prazo, quantificação de pacientes beneficiados, critérios de elegibilidade, desfechos de saúde, limites anuais de custeio e regras de interrupção, com reavaliação periódica. A implementação depende de fatores como a Lei de Licitações (Lei 14.133/2021), que admite diálogos competitivos, alocação de riscos e remuneração por desempenho.

Infraestrutura digital é essencial, pois acordos mais complexos exigem registros de pacientes e monitoramento. Em conclusão, reformar o Estado para melhorar a eficiência na gestão pública e privada é necessário; o ACR oferece acesso com avaliação de qualidade e sustentabilidade. Como disse Jean Tirole, reformar o Estado é colocar a economia a serviço do bem comum.

Assim, o Fórum Permanente atuou de forma colaborativa no desenvolvimento de diretrizes que atendem ao artigo 50 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), demonstrando o alinhamento do setor com a governança de dados e a segurança das informações de seus titulares e oferecendo um conjunto robusto de orientações para o setor.

Nesse sentido, o Fórum monitorou de perto a evolução da legislação e suas interpretações, identificando os principais desafios e propondo soluções práticas que contribuem para a conformidade e promovem a inovação nos serviços de saúde, traduzindo essas novas perspectivas nesta versão atualizada.

O Código está organizado em duas partes. A primeira abrange regulamentações e conceitos essenciais da LGPD aplicados ao setor de saúde. A segunda oferece diretrizes práticas para a aplicação da lei, com foco na proteção de dados sensíveis e na promoção de uma cultura de segurança da informação, inovação e respeito aos direitos dos titulares.

Assim, este Guia reafirma o compromisso do setor de saúde com a proteção de dados, proporcionando diretrizes práticas que garantem o exercício dos direitos dos titulares e fomentam o desenvolvimento tecnológico, científico e econômico de Prestadores de Serviço de Saúde, Operadoras de Planos de Saúde e Fornecedores de Produtos para Saúde.

CISCO Secure. Privacy's Growing Importance and Impact - Data Privacy Benchmark Study. 2023.
Disponível em: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2023.pdf. Acesso em: 17 de abril de 2024.

2. ÂMBITO DE APLICAÇÃO

Este Guia foi elaborado com base na atuação de três grupos principais: (i) Prestadores de Serviços de Saúde (Hospitais e SADTs - Serviços Auxiliares de Diagnóstico e Terapia), (ii) Operadoras de Planos de Saúde e (iii) Fornecedores e Distribuidores de Produtos para Saúde.

Os Prestadores de Serviços de Saúde incluem tanto instituições lucrativas quanto filantrópicas, como hospitais, clínicas, laboratórios e outros estabelecimentos que realizam atividades como consultas, cirurgias e tratamentos terapêuticos, além dos profissionais responsáveis. Independente do porte, todas essas entidades desempenham um papel fundamental na promoção da saúde, prevenção de doenças, diagnóstico e tratamento, bem como no suporte contínuo ao paciente durante todo o processo de recuperação.

As Operadoras de Planos de Saúde garantem o acesso a serviços médicos, hospitalares e odontológicos no setor privado. Elas atuam como intermediárias entre os prestadores de serviços e os beneficiários, coordenando autorizações de procedimentos e a rede de atendimento.

Por fim, os Fornecedores e Distribuidores de Produtos para Saúde são responsáveis pela entrega de equipamentos e dispositivos essenciais, como instrumentos cirúrgicos, órteses, próteses e materiais especiais (OPME) produtos médicos, aparelhos, implantes, materiais, artigos, equipamentos de proteção individual (EPIs) e sistemas de alta tecnologia, como ressonância magnética, atuando na cadeia de abastecimento da saúde. Eles garantem que os recursos necessários estejam disponíveis para a atuação dos profissionais de saúde, contribuindo para a continuidade dos serviços de forma eficaz e segura.

Diante da diversidade de entidades envolvidas, o Guia identifica desafios comuns quanto à aplicação da LGPD no setor, padronizando e alinhando boas práticas e recomendações de conformidade, de forma que elas se adaptem aos diferentes perfis e portes dos agentes de tratamento de dados.

3. A PROTEÇÃO DE DADOS NO SETOR DA SAÚDE E AS FINALIDADES DE TRATAMENTO

De acordo com a LGPD, tratamento de dados pessoais significa qualquer "operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (Art. 5º, X).

Os três principais representantes do setor — Prestadores de Serviço de Saúde, Operadoras de Planos de Saúde e Fornecedores de Produtos para Saúde — compartilham várias atividades relacionadas ao tratamento de dados. Por exemplo: gestão de pessoal e recursos humanos, administração de contratos com clientes e parceiros, auditorias, e cumprimento de obrigações legais e regulatórias. Ainda assim, existem algumas particularidades de cada um deles que merecem ser destacadas.

FENASAÚDE. Somos a FenaSaúde. Disponível em: https://fenasaude.org.br/. ABRAMGE. Quem Somos. Disponível em: https://abramge.com.br/quem-somos/..

ABRAIDI. O Setor de Produtos para Saúde. Disponível em: https://abraidi.com.br/entenda-o-setor-de-produtos-para-saude/.

PRESTADORES DE **SERVIÇOS DE SAÚDE**

- Atendimento médico, inclusive modalidades de telessaúde.
- Uso de dados (resultados de exames, histórico do paciente) para diagnóstico e tratamento.
- Emissão de laudos.
- Agendamento de consultas.
- Gestão de leitos e recursos.
- Pesquisa clínica e Programas de Suporte ao Paciente, ensino e treinamento.
- Compartilhamento de dados (resultados de exames, histórico) entre médicos e corpo clínico.
- Compartilhamento com operadoras de saúde para faturamento, elegibilidade, coordenação de cuidado e auditoria médica.
- Compartilhamento com autoridades regulatórias.
- Uso de WhatsApp e softwares para troca de informações sobre cirurgias.
- Realização de exames laboratoriais e análise de amostras.

- Emissão de laudos.
- Armazenamento de resultados para consulta e pesquisa.
- Armazenamento de prontuários para cumprimento de obrigações regulatórias.
- Monitoramento de indicadores de qualidade (como taxas de infecção hospitalar).
- Compartilhamento com médicos e hospitais para diagnóstico e/ou tratamento.
- Envio de comunicações transacionais de procedimentos e de relacionamento com o paciente.
- Pesquisas de satisfação e desenvolvimento de novos produtos e serviços.

OPERADORAS DE **PLANOS DE SAÚDE**

- Gestão de contratos para realização de tratativas prévias à contratação.
- Autorização de procedimentos.
- Agendamento de consultas e exames.
- Envio de comunicações sobre produtos e serviços aos clientes.
- Prestação de atendimento por canais como a Ouvidoria e Centrais de Atendimento ao cliente.
- Análise de dados para gestão de riscos.
- Desenvolvimento de produtos e serviços.
- Compartilhamento de dados pelo padrão TISS (ANS).
- Compartilhamento de dados para cobrança em casos de coparticipação.
- Compartilhamento de dados para cálculo de preços pós-estabelecidos.
- Dados sobre atendimentos médicos, receitas, atestados e acompanhamento médico.
- Análise de dados atuariais.
- Tratamento de dados para prevenção à fraude.
- Cumprimento de obrigações regulatórias (como as normas da ANS, ANVISA, entre outros).
- Compartilhamento de dados para gestão de saúde populacional.

FORNECEDORES E DISTRIBUIDORES DE **PRODUTOS PARA SAÚDE**

- Fornecimento de dispositivos médicos, incluindo coleta de dados para suporte pré-cirurgia (tal como para definição prévia das especificidades de um dispositivo implantável) e pós-cirurgia, bem como para melhorias de produtos.
- Desenvolvimento de aplicativos e plataformas com cadastro de dados pessoais.
- Uso de WhatsApp e softwares para troca de informações sobre cirurgias.
- Emissão de Notas Fiscais.[4]
- Rastreamento de dispositivos médicos e dossiês dos dispositivos.
- Compartilhamento de dados do paciente e profissional de saúde para cotação, remessa e faturamento.
- Compartilhamento de dados em caso de reclamação de produto para análise e ação.
- Compartilhamento de dados com planos de saúde para autorização de procedimentos e faturamento.
- Acompanhamento de procedimentos cirúrgicos por assessor técnico que fornece orientações sobre o uso adequado dos materiais e equipamentos, além de assistência na montagem de dispositivos médicos.
- Troca de dados com instrumentadores para agendamento de cirurgias e relatórios de consumo.
- Acesso a dados de pacientes para manutenção de dispositivos.
- Participação em eventos com profissionais de saúde (HCPs) e interação científica.
- Compartilhamento de dados com autoridades regulatórias (Anvisa).

As particularidades das operações de tratamento de dados de cada um dos grupos representados no Fórum não impedem que essas atividades sejam frequentemente integradas. A título de exemplo, os fornecedores de produtos para saúde podem faturar tais produtos tanto para o plano de saúde quanto para o hospital ou para o paciente, titular de dados. Ou seja, o procedimento pode ser solicitado pelo profissional de saúde, que também especifica o material necessário para o implante. A aprovação do procedimento e a disponibilização do material passam pela operadora de saúde, que autoriza o hospital a receber o material do fabricante ou importador e o disponibiliza para o procedimento, beneficiando o paciente, titular dos dados. Caso o paciente não possua plano de saúde, os dispositivos médicos podem, também, ser fornecidos pelos fornecedores e distribuidores de produtos para saúde diretamente ao paciente ou ao hospital.

A ilustração abaixo demonstra um fluxo de dados pessoais no setor de saúde, destacando as interações entre Prestadores de Serviço de Saúde, Operadoras de Planos de Saúde e Fornecedores de Produtos para Saúde.

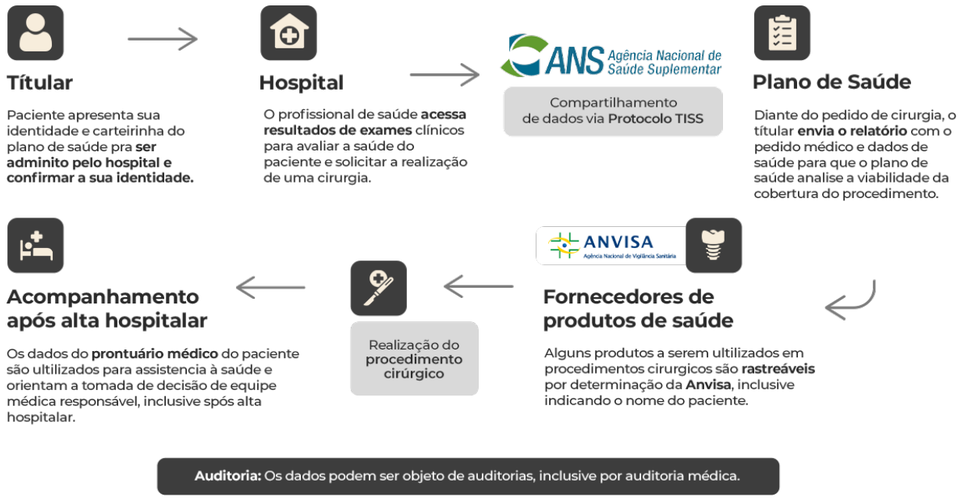


Figura 1: Exemplo do fluxo de dados pessoais para atendimento do paciente com indicação de cirurgia.

4- Existem desafios sobre o tratamento de dados pessoais neste setor. Como exemplo, cabe indicar a Portaria nº 0817/SES, de 5 de agosto de 1996, do Estado de Santa Catarina, que determina a obrigatoriedade de constar na Nota Fiscal referente à realização do procedimento que envolver órteses, próteses e materiais especiais, dados pessoais do paciente (nome). Esta informação deve ser acompanhada das demais relativas especificamente ao procedimento realizado (a data do uso, o médico responsável, o hospital em que foi atendido, procedimento realizado (código tabela SIH/SUS), descrição do material, quantidade, valor unitário e o valor total do material utilizado/implantado).

Esse exemplo de tratamento de dados no setor de saúde ilustra a complexidade das relações entre os diversos atores envolvidos e reforça a importância da adoção de programas de compliance efetivos, além da avaliação contínua das melhores práticas relacionadas à LGPD. É nesse contexto que este guia se propõe a oferecer diretrizes claras e práticas para a proteção de dados no setor de saúde, levando em conta as particularidades na interpretação de conceitos, obrigações e diretrizes estabelecidas pela legislação.

4. CONCEITOS DA LEI GERAL DE PROTEÇÃO DE DADOS APLICADOS AO SETOR DA SAÚDE

A LGPD estabeleceu no Brasil um marco geral para a proteção de dados pessoais, permitindo que os titulares exerçam efetivamente seus direitos em relação ao tratamento de seus dados. A lei define princípios, direitos dos titulares e mecanismos de responsabilidade para garantir a proteção dos dados e fornecer segurança jurídica ao mercado e ao setor público no uso adequado dessas informações.

Nesse sentido, esta seção aborda importantes conceitos de proteção de dados aplicados ao setor de saúde, incluindo as principais categorias de dados pessoais envolvidos e a definição de agentes de tratamento.

Em relação ao primeiro aspecto, destaca-se que a lei adota um conceito amplo de dados pessoais. Para a LGPD, é dado pessoal qualquer "informação relacionada a pessoa natural identificada ou identificável" (Art. 5º, I). Ou seja, são classificados como dados pessoais, inclusive, aquelas informações que podem levar à identificação do seu titular, mesmo que não estejam diretamente relacionadas a ele. Os dados de pessoas jurídicas, por regra, não são dados pessoais.

DADOS ANONIMIZADOS E DADOS PSEUDONIMIZADOS

É importante notar que, embora o conceito de dados pessoais seja alargado, se os dados forem anonimizados eles não são considerados dados pessoais. Segundo a lei, o dado anonimizado é: "dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (art.5º, II, da LGPD). O processo de anonimização, segundo a lei, é: a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (Art. 5º, XI).

Ainda, é possível que dados pessoais passem por um processo de pseudonimização, que não permite a identificação direta dos titulares, mas que não extingue completamente essa possibilidade, ou seja, um "tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro" (Art. 13, §4º). Nesse caso, o dado pseudonimizado não perde a característica de dado pessoal, os requisitos da LGPD ainda devem ser observados, mas o risco associado ao tratamento desse dado é minimizado.

As técnicas de anonimização e pseudonimização são ferramentas interessantes para implementação de boas práticas no tratamento de dados pessoais. Especialmente as técnicas de anonimização, são essenciais para viabilizar o fluxo de dados para finalidades de inovação em saúde, tais como:

(a) o desenvolvimento de pesquisas por entes com fins lucrativos – que não se encaixam na hipótese legal de realização de estudos por órgão de pesquisa do artigo 11, II, (c);

(b) a criação de bases de dados comuns para desenvolvimento, treinamento e validação de novas tecnologias como aquelas envolvendo inteligência artificial;

(c) a elaboração de dados analíticos agregados sobre o uso dos serviços de saúde ("Analytics").

Assim, a anonimização robusta é alternativa que pode oferecer menor risco para realizar esse tipo de operação de forma legitima, sem comprometer os direitos dos titulares.

Por fim, vale destacar o risco de reidentificação, ou seja, de um dado considerado anonimizado, ou mesmo pseudonimizado, ser processado de forma a permitir a vinculação do dado com uma pessoa.

A própria ANPD reconhece que "a anonimização deve ser entendida como um processo contínuo baseado em riscos, composto por muitas fases e com transições multidirecionais entre essas [...], não sendo factível considerar que o processo de anonimização pode resultar em um cenário de risco zero".

Portanto, as práticas de anonimização e pseudonimização devem ser implementadas sob a perspectiva de minimização dos riscos do tratamento, mas não de eliminação destes. Todo esse processo deve ser documentado através de relatórios que devem ser produzidos no contexto no qual se realiza a operação de anonimização.

Além disso, a distinção entre dados sensíveis e não sensíveis é fundamental para orientar a análise de riscos pelos responsáveis pelo tratamento, já que os dados de saúde são considerados sensíveis. Essa classificação também é essencial para garantir a correta aplicação das condições

de legitimidade para o tratamento, conforme os princípios e requisitos legais estabelecidos na lei, que será abordado em detalhes no próximo tópico.

Ainda que a LGPD não apresente de forma explícita o conceito de dado pessoal sensível de saúde, esse compreende também as informações relacionadas à saúde física ou mental de uma pessoa. O Regulamento Geral de Proteção de Dados europeu (RGPD) define o conceito de "dados relativos à saúde" como "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de cuidados de saúde, que revelem informações sobre o seu estado de saúde" (Art. 4º (15)).

ANPD. Estudo técnico sobre anonimização de dados na LGPD: uma visão de processo baseado em risco e técnicas computacionais. 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/estudo_tecnico_sobre_anonimizacao_de_dados_na_lgpd_uma_visao_de_processo_baseado_em_risco_e_tecnicas_computacionais .pdf.

Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho de 27 de abril de 2016. Tradução livre.

DADOS PESSOAIS EM **ATESTADO MÉDICO**

No atestado médico, por exemplo, há informações que permitem a identificação do paciente, como o nome e a data de nascimento, classificadas como dados pessoais (Art. 5º, I, da LGPD). Nessa categoria também estão inclusos os dados que permitem a identificação do profissional responsável pelo seu atendimento (como o nome e informações profissionais – no caso de médicos, os números vinculados ao CRM).

O atestado também pode conter informações sobre a condição de saúde do titular. Se autorizado expressamente pelo paciente ou seu representante legal, o médico poderá indicar o diagnóstico neste documento (Art. 5º, § 4º da Resolução CFM nº 2381/2024), o que se caracteriza como dado pessoal sensível pois relativo à saúde do paciente (Art. 5º, II, da LGPD).

AUTORIZAÇÃO DE EXAMES PELAS OPERADORAS DE PLANO DE SAÚDE

Os pacientes beneficiários de um plano de saúde passam por um processo de autorização de exames ou procedimentos quando utilizam um serviço. O objetivo dessa autorização é verificar se o procedimento que o paciente quer realizar está coberto ou não pelo plano contratado, inclusive se o procedimento está na lista de cobertura mínima obrigatória determinada pela ANS.

Para que a operadora autorize a realização do procedimento, ela coleta informações pessoais, como nome, CPF, número da carteirinha do plano e pedido médico a fim de analisar a incidência do período de carência, a cobertura contratual e a cobertura mínima do rol da ANS. Nesse caso, o tratamento de informações pessoais é fundamental para que a autorização seja garantida ao beneficiário.

UTILIZAÇÃO DE ETIQUETAS DE RASTREABILIDADE POR DISTRIBUIDORES E FORNECEDORES DE PRODUTOS PARA SAÚDE

A Nota Técnica nº 19/2020/SEI/CMIOR/GEMAT/GGTPS/DIRE3/ANVISA, no processo nº 25351.905512/2020-67, indica para a necessidade de tratamento de dados pessoais nos casos de desenvolvimento de dispositivos médicos personalizados fabricados sob medida. Nesses casos, a RDC n. 305/2019 descreve que as etiquetas de rastreabilidade fornecidas pelo fabricante ou importados "devem conter identificação do produto, seguido de indicação 'dispositivo médico sob medida'; identificação do fabricante nacional ou importador (CNPJ e Razão Social); número de rastreio do produto; identificação do paciente (iniciais do nome completo); e identificação do profissional de saúde responsável, seguido do número de inscrição no conselho profissional". Dessa forma, no fornecimento de produtos para saúde personalizados, o tratamento de dados de nome e número de inscrição no conselho profissional é necessário. A ANVISA ainda afirma que esses dados "são fornecidos ao fabricante (nacional) ou importador na fase de projeto do produto". Na mesma linha, a RDC nº 556/2021 também prevê etiqueta de rastreabilidade para produtos implantáveis, a ser disponibilizada pelo fabricante ou importador no prontuário clínico, no documento a ser entregue ao paciente e na documentação fiscal que gera a cobrança, com identificação de cada material ou componente de sistema implantável.

Já o conceito de agentes de tratamento, segundo a LGPD, envolve duas figuras: o controlador e o operador (Art. 5º, VI e VII). A identificação de ambos é crucial para a atribuição de responsabilidades e deve ser feita de acordo com o contexto de cada atividade de tratamento de dados. A principal diferença entre essas funções está no poder de decisão, que caracteriza o papel do controlador, responsável por definir os elementos essenciais para o cumprimento das finalidades do tratamento.

O Guia Orientativo para a Definição dos Agentes de Tratamento e do Encarregado da ANPD traz exemplos específicos do setor de saúde para ilustrar a distinção entre essas funções e a correta identificação do controlador e do operador em diferentes contextos.

IDENTIFICAÇÃO DO PAPEL DE CONTROLADOR **GUIA DA ANPD**

Profissionais de saúde, como médicos, podem ser identificados ou não como agentes de tratamento a depender do contexto. No caso de atuação profissional liberal, em que o médico trata, seja coletando, manipulando ou armazenando, dados pessoais do paciente em seu consultório, como os prontuários, o profissional será identificado como controlador. Entretanto, caso possua vínculo de emprego com um hospital e atue como "principal representante do hospital junto a um serviço de armazenamento de dados de pacientes em nuvem, inclusive assinando os contratos correspondentes", o profissional não será identificado como agente de tratamento, mas sim o hospital, que é o controlador neste caso

Tanto o controlador quanto o operador podem ser pessoas físicas ou jurídicas, de direito público ou privado. A identificação do controlador deve levar em conta o contexto e as circunstâncias do caso, podendo estar prevista em contrato entre as partes que pode prever também as obrigações e responsabilidades de cada um dos agentes de tratamento. O controlador é responsável mesmo que não realize diretamente qualquer operação de tratamento. Além disso, uma mesma organização pode atuar como controladora e operadora, dependendo das atividades de tratamento que realiza.

O tratamento de dados também pode envolver uma controladoria conjunta, comum ou convergente. Isso ocorre quando dois ou mais controladores definem em conjunto as finalidades e os elementos essenciais do tratamento de dados pessoais, tendo um interesse mútuo sobre o tratamento. De acordo com a ANPD, esses elementos essenciais incluem a definição das categorias de titulares, os dados pessoais envolvidos, a base legal aplicável e o período de armazenamento. Nesses casos, os controladores conjuntos têm responsabilidade solidária, o que destaca a importância de todos os agentes do fluxo de tratamento de dados estarem em conformidade com a LGPD. Se as finalidades do tratamento forem distintas, não haverá controladoria conjunta, mesmo que os dados tratados sejam os mesmos.

Além disso, o operador pode contratar um suboperador para auxiliá-lo no tratamento de dados pessoais em nome do controlador. No entanto, a relação direta do suboperador é com o operador, não com o controlador. Por isso, é recomendável

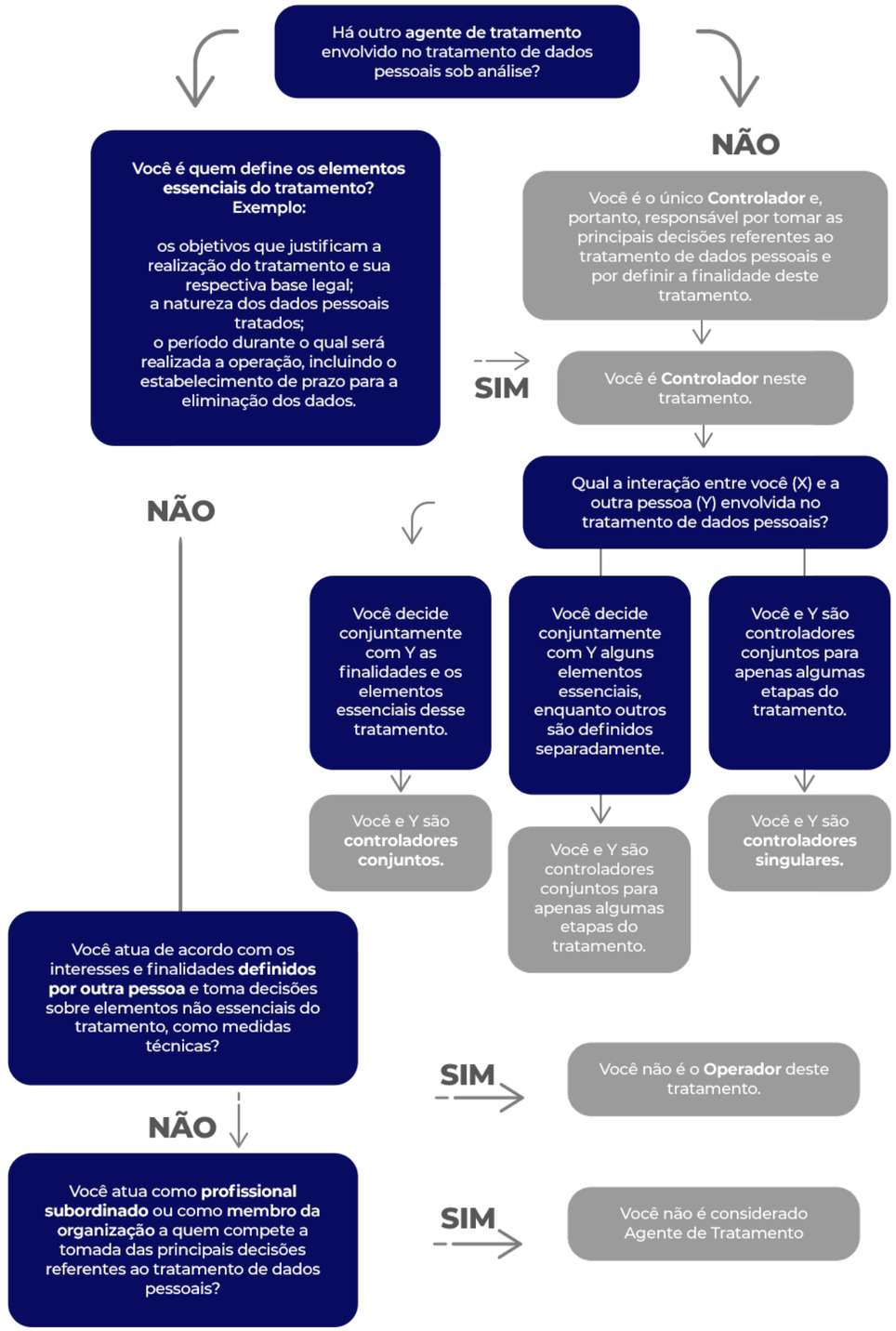
que o operador obtenha autorização formal do controlador para contratar o suboperador, evitando que essa contratação seja interpretada como uma ação que viole as diretrizes do controlador, o que poderia resultar em responsabilidade solidária entre o operador e o suboperador.

Em relação aos representantes do Fórum, podemos identificar as seguintes hipóteses nas quais cada um poderia figurar como agentes de tratamento:

AGENTE DE TRATAMENTO	DESCRIÇÃO DO TRATAMENTO
Controlador: Rede Hospitalar Saúde **Operador:** Empresa de Software de PPE	*A Rede Hospitalar Saúde coleta e mantém registros médicos dos pacientes e é responsável por determinar como esses dados são usados e protegidos. A Rede Hospitalar contrata uma Empresa de Software de Provedor de Prontuário Eletrônico (PPE) para fornecer a infraestrutura técnica para armazenar e gerenciar esses registros eletronicamente. A empresa de PPE processa os dados de acordo com as instruções do hospital, mas não toma decisões sobre seu uso.*
Controlador: Companhia de Seguro de Saúde **Operador:** Serviço Terceirizado de Processamento de Sinistros	*Uma companhia de plano de saúde coleta informações dos segurados e dados de sinistros médicos. Eles terceirizam o processamento de sinistros para um serviço especializado. A companhia decide quais dados são coletados e como são usados para decisões de cobertura, enquanto o serviço de processamento de sinistros segue diretrizes estritas no manuseio dos dados para processar os sinistros de forma eficiente.*
Controlador: Fornecedor e Distribuidor de Produtos de Saúde **Operador:** Empresa de armazenamento em nuvem	*Uma empresa de fornecimento de produtos de saúde personalizados trata dados pessoais do médico solicitante do produto para atender normas de rastreabilidade da ANVISA. Para tanto, ela mantém uma lista com nome de médicos e números de registro em suas bases de dados. Essas bases são armazenadas por um provedor de armazenamento de dados em nuvem, que atua como operadora dos dados pessoais tratados pela empresa que fornece o produto.*

Para auxiliar na identificação dos agentes, a ANPD apresentou explicações no "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado" e fornece o seguinte organograma a respeito da aplicação desses conceitos:

ANPD. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. 2022. P. 25. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf.



Para tanto, o encarregado deve ser o agente capaz de se comunicar com os titulares e com a ANPD, de forma clara, precisa e em língua portuguesa (Art. 13, da Resolução CD/ANPD nº 18/2024).

Apesar de não ser um agente de tratamento, a LGPD apresenta o encarregado pelo tratamento de dados pessoais como ator fundamental para garantir a proteção de dados. O encarregado e o seu substituto devem ser indicados por ato documental do controlador (Art. 41, da LGPD) e ter as suas identidades (como os seus nomes) e as informações de contato (como os seus e-mails e/ou números e/ou canal oficial para atendimento que viabilizem o "exercício dos direitos dos titulares junto ao controlador e possibilitem o recebimento de comunicações da ANPD" - Art. 9º, §2º, da Resolução CD/ANPD nº 18/2024) divulgadas no sítio eletrônico do controlador de forma pública, clara, objetiva e com destaque (Art. 41, §1º, da LGPD e Art. 9º, da Resolução CD/ANPD nº 18/2024).

Para a divulgação da identidade do encarregado e do substituto, o controlador deverá compartilhar no mínimo no sítio eletrônico ou, caso este não exista, em "quaisquer outros meios de comunicação disponíveis, especialmente aqueles usualmente utilizados para contato com os titulares" (Art. 9º, §3º, da Resolução CD/ANPD nº 18/2024):

o nome completo, se for pessoa natural (Art. 9º, §1º, I, da Resolução CD/ANPD nº 18/2024), ou;

o nome empresarial ou o título do estabelecimento, bem como o nome completo da pessoa natural responsável, se pessoa jurídica Art. 9º, §1º, II, da Resolução CD/ANPD nº 18/2024).

Como regra geral, espera-se que toda organização indique uma pessoa (natural ou jurídica) para assumir esse papel, diante da sua relevância em atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. Para instituições de pequeno porte, é dispensada a indicação de encarregado e, nestes casos, devem disponibilizar um canal de comunicação com o titular, conforme Art. 11 do Regulamento de aplicação da LGPD (Resolução CD/ANPD nº 2/2022).

O encarregado poderá contribuir com a indicação de quais ações devem ser adotadas, em consideração ao volume de dados e necessidade de cada organização, e exercer as seguintes atribuições previstas nos artigos 15 e 16 da Resolução CD/ANPD nº 18/2024:

ATRIBUIÇÕES DO ENCARREGADO (CD/ANPD Nº 18/2024)

Atividades do encarregado:

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências (Art. 15, I).
- Receber comunicações da ANPD e adotar as providências necessárias (Art. 15, II).
- Orientar funcionários e contratados sobre práticas de proteção de dados pessoais (Art. 15, III).
- Executar outras atribuições definidas pelo agente de tratamento ou estabelecidas em normas complementares (Art. 15, IV).

Ao receber comunicações da ANPD, o encarregado deve:

- Encaminhar a demanda internamente para as unidades competentes (Art. 15, § único, I).
- Fornecer orientação e assistência necessárias ao agente de tratamento (Art. 15, § único, II).
- Indicar o representante do agente de tratamento perante a ANPD, quando não for o próprio encarregado (Art. 15, § único, III).

O encarregado deve colaborar, conforme solicitado, com a elaboração, definição e implementação dos seguintes processos e documentos (Art. 16):

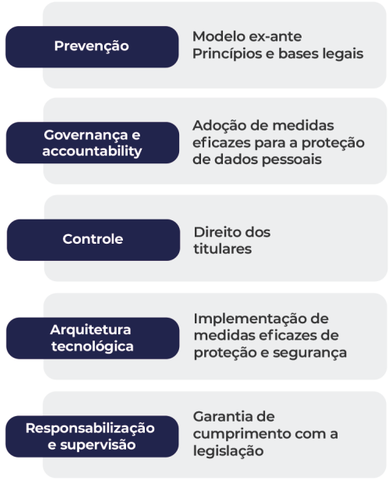
- Registro e comunicação de incidentes de segurança (Art. 16, I).
- Registro das operações de tratamento de dados pessoais (Art. 16, II).
- Relatório de impacto à proteção de dados pessoais (Art. 16, III).
- Mecanismos de supervisão e mitigação de riscos no tratamento de dados pessoais (Art. 16, IV).
- Medidas de segurança para proteger dados pessoais de acessos não autorizados ou incidentes ilícitos ou acidentais (Art. 16, V).
- Políticas internas que assegurem o cumprimento da LGPD e regulamentos da ANPD (Art. 16, VI).
- Instrumentos contratuais que tratem do tratamento de dados pessoais (Art. 16, VII).
- Transferências internacionais de dados (Art. 16, VIII).
- Regras de boas práticas e governança em privacidade, conforme o Art. 50 da LGPD (Art. 16, IX).
- Produtos e serviços com design compatível com os princípios da LGPD, incluindo privacidade por padrão e limitação de coleta de dados ao mínimo necessário (Art. 16, X).
- Outras atividades e decisões estratégicas relacionadas ao tratamento de dados pessoais (Art. 16, XI)

Destaca-se que para as atividades mencionadas acima e perante a ANPD, o encarregado não será responsabilizado pela conformidade do tratamento de dados realizado pelo controlador (Art. 17, da Resolução CD/ANPD nº 18/2024).

O encarregado pode ser tanto um empregado da instituição quanto um agente externo, de natureza física ou jurídica e deve ser indicado por um documento, ato formal do agente de tratamento, que deve ser apresentado à ANPD se assim solicitado (Art. 3º, §1º e §2º, da Resolução CD/ANPD nº 18/2024). Este documento deve ser "escrito, datado e assinado, que, de maneira clara e inequívoca, demonstre a intenção do agente de tratamento em designar como encarregado uma pessoa natural ou uma pessoa jurídica" (Art. 3º, §1º, da Resolução CD/ANPD nº 18/2024).

5. CONDIÇÕES DE LEGITIMIDADE PARA O TRATAMENTO DE DADOS PESSOAIS NA ÁREA DA SAÚDE

A LGPD é uma lei estruturada em cinco pilares fundamentais que buscam a concretização do direito fundamental à proteção de dados pessoais. Os cinco pilares são:



Sistema desenvolvido e estruturado por Laura Schertel Mendes.

Quanto à "governança e accountability", trata-se de previsão que está insculpida no Art. 6º, inciso, X, que versa sobre a "responsabilização e prestação de contas". Essa previsão apresenta a obrigação de "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".

Assim, a LGPD determina que empresas e órgãos públicos devem demonstrar que estão tomando medidas eficazes para cumprir a lei. Isso inclui práticas de prestação de contas sobre as ações adotadas para proteger os dados pessoais, como a nomeação de um encarregado de proteção de dados e a implementação de um programa de governança de dados. Ademais, buscando fortalecer as iniciativas dos agentes de tratamento para implementação de programas de compliance de dados efetivos, o Art. 50 da LGPD apresenta a possibilidade de que os agentes de tratamento formulem medidas de governança de dados que possibilitem o cumprimento da legislação.

No aspecto do "controle", a LGPD coloca o titular dos dados no centro, concedendo-lhe vários direitos para gerenciar suas próprias informações. Entre esses direitos, que serão detalhados no tópico VIII, estão os previstos nos Arts. 17 a 22 da Lei.

A "arquitetura tecnológica" exige que as medidas de proteção e segurança sejam adequadas à natureza dos dados e aos riscos do tratamento, desde a concepção dos sistemas. Essas medidas refletem o previsto no Art. 46 da LGPD que exige que os agentes de tratamento adotem "medidas de segurança, 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".

Por fim, a LGPD estabelece um sistema robusto de "responsabilização e supervisão" para garantir o cumprimento da lei e a proteção dos dados pessoais. As sanções estabelecidas pelo Art. 52 da LGPD incluem uma gama variada de penalidades, tais como advertências, multas, e até a suspensão parcial ou total das atividades relacionadas ao tratamento de dados.

PENALIDADES PREVISTAS NA LGPD

- advertência, com indicação de prazo para adoção de medidas corretivas;
- multa simples e multa diária, observando o limite 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;
- 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 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; e
- proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Inclusive, em julho de 2023, a ANPD aplicou a sua primeira sanção por descumprimento à LGPD. A atuação fiscalizatória da Autoridade é feita pela Coordenação-Geral de Fiscalização (CGF) e se dá com base em uma regulação responsiva que privilegia a adoção de medidas de monitoramento, orientação e prevenção, além das ações de repressão, buscando mensurar a sanção proporcional à desconformidade percebida.

Assim, a depender da infração à LGPD, a empresa pode estar submetida a uma série de recomendações da autoridade, além da atividade sancionatória em que a empresa fiscalizada é condenada por uma infração à LGPD. Nos processos sancionatórios, o Regulamento de Dosimetria permite mensurar a sanção adequada para cada tipo de infração.

ANPD aplica a primeira multa por descumprimento à LGPD. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd. Acesso em: 25 de abril de 2024.

ANPD. Fiscalização. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-como_fisalizamos?

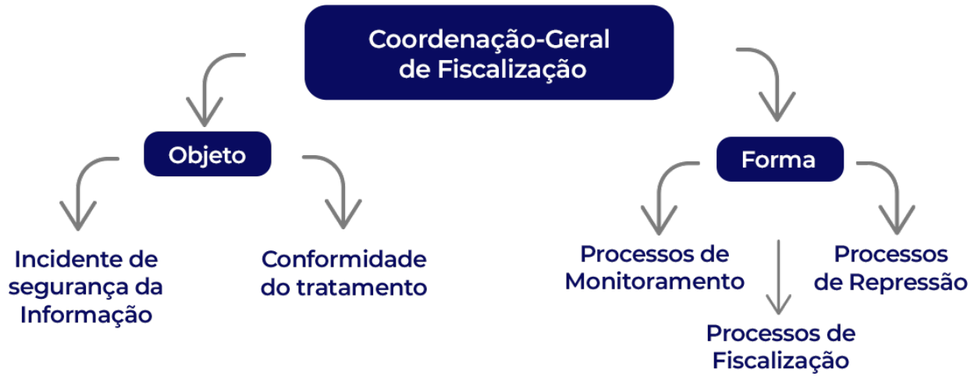


Figura 2: Atividades de Fiscalização da ANPD

As atividades de fiscalização da ANPD também são orientadas pelo Mapa de Temas Prioritários, documento elaborado pela Coordenação-Geral de Fiscalização para planejar as atividades de controle com base em critérios de risco, a gravidade, a atualidade e a relevância. Estar atento aos temas de fiscalização da ANPD permite que o setor de saúde se antecipe de possíveis ações que deve implementar para evitar ser surpreendido na fiscalização da autoridade.

A ANPD já aplicou algumas sanções a entes públicos e privados, sendo que, dentre os entes públicos, há alguns que atuam no setor de saúde, como a Secretaria Estadual de Saúde de SC e o próprio Ministério da Saúde.

Ademais, os agentes de tratamento que causarem dano patrimonial, individual ou coletivo nos termos do Art. 42 da LGPD também se sujeitam à reparação dos danos causados junto ao judiciário, sendo aplicável as disposições do Código Civil. Dessa forma, o Poder Judiciário também pode ser acionado em casos que tratam de responsabilização civil.

Os próximos tópicos irão explorar com mais detalhes os componentes do primeiro pilar, que trata das condições de legitimidade para o tratamento de dados pessoais dos titulares, com foco nas bases legais e princípios definidos pela LGPD. Já os demais pilares serão abordados na Parte II, que será dedicada às melhores práticas a serem adotadas no setor.

ANPD. Resolução CD/ANPD nº 1, de 28 de outubro de 2021. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd_anpd-no-1-de-28-de-outubro-de-2021.pdf

https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-comofisalizamos?

5.1 PRINCÍPIOS APLICÁVEIS

A LGPD estabelece onze princípios que orientam todas as fases do tratamento de dados pessoais, conforme o artigo 6º. Esses princípios, juntamente com as bases legais, formam o pilar da legitimidade do tratamento de dados pessoais e, por isso, devem ser considerados em todas as etapas do processo.

PRINCÍPIOS DA **LGPD**

Boa-Fé objetiva **(Art. 6º, caput)**	*A necessidade de que os tratamentos de dados pessoais sejam pautados pelo caráter cooperativo e lisura na relação dos agentes com o titular, que deve ser passível de constatação a partir de atos objetivos.*
Finalidade **(Art. 6º, I)**	*O tratamento deve ser feito para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.*
Adequação **(Art. 6º, II)**	*Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.*
Necessidade **(Art. 6º, III)**	*Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos.*
Livre Acesso **(Art. 6º, IV)**	*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 **(Art. 6º, V)**	*Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade do tratamento.*
Transparência **(Art. 6º, VI)**	*Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre o tratamento e os respectivos agentes responsáveis, observados os segredos comercial e industrial.*
Segurança **(Art. 6º, VII)**	*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 **(Art. 6º, VIII)**	*Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.*
Não discriminação (Art. 6º, IX)	*Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.*
Responsabilização e prestação de contas (Art. 6º, X)	*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.*

Os princípios da LGPD oferecem maior segurança e direcionamento para as organizações que tratam dados pessoais, além de garantir ao titular maior controle sobre suas informações. Entre os princípios, destacam-se o da finalidade e o da necessidade, que exigem uma avaliação cuidadosa do motivo pelo qual os dados são tratados, a legitimidade do objetivo almejado com o tratamento e da extensão dos dados realmente necessários para essa finalidade.

Já o princípio da transparência (Art. 6º, VI) assegura que os titulares tenham acesso a informações claras, precisas e facilmente acessíveis sobre as atividades de tratamento e os responsáveis por elas, respeitando os segredos comercial e industrial. Esse princípio é fundamental e se reflete em diversos artigos da LGPD, como nos direitos garantidos aos titulares, exigindo que todas as informações sobre o processamento de dados sejam acessíveis e compreensíveis. Isso pode ser viabilizado pela disponibilização de avisos ou políticas de privacidade que detalhem de forma clara como os dados são tratados, por exemplo:

POLÍTICA DE **PRIVACIDADE**

- **Introdução e Escopo:** Objetivo da política de privacidade. Visão geral do compromisso da empresa com a proteção de dados. Âmbito de aplicação da política de privacidade (por exemplo, site, aplicativo móvel, serviços presenciais, serviços por telefone).
- **Tipos de Dados Pessoais Coletados:** Dados de cadastro e contato. Informações demográficas. Informações de saúde do paciente, como pedidos médicos, resultado de exames, diagnósticos, registros e atestados. Informações de seguro de saúde e histórico de consultas. Informações de produtos de saúde adquiridos. Dados de uso do site da empresa.
- **Métodos de Coleta de Dados:** Coleta direta dos pacientes. Coleta automatizada através do uso do site/aplicativo. Fontes de terceiros (por exemplo, médicos de referência, raspagem de dados na internet, recebimento de dados de terceiros).
- **Finalidades do Processamento de Dados:** Realização de exames, consultas, cirurgias e acompanhamento desses serviços de saúde. Envio de documentos por correio ou correio eletrônico. Faturamento e cobrança do pagamento. Agendamento de consultas. Comunicações de marketing (se aplicável). Prestação de assistência e atendimento ao paciente após o serviço de saúde.
- **Políticas de Retenção de Dados:** Duração do armazenamento de dados. Critérios para determinar os períodos de retenção.
- **Compartilhamento de Dados e Divulgações a Terceiros:** Prestadores de serviços de saúde. Operadoras de Planos de Saúde. Fornecedores e Distribuidores de Produtos de Saúde. Agências reguladoras e órgão públicos (conforme exigido por lei). Autoridade judiciária (após decisão judicial). Prestadores de serviços (por exemplo, TI, faturamento).
- **Direitos dos Titulares:** Espécies de direitos que podem ser exercidos pelos titulares. Canal de comunicação para exercício desses direitos. Possibilidade de peticionamento perante a ANPD se a resposta não for satisfatória.
- **Transferência Internacional:** forma, a duração e a finalidade específica da transferência internacional, além de país de destino dos dados transferidos.

Dado o desafio de se assegurar adequadamente a aplicação dos princípios da LGPD, algumas perguntas podem auxiliar os responsáveis pelo tratamento na análise das suas decisões:

PERGUNTAS QUE **PODEM ORIENTAR** A APLICAÇÃO DOS PRINCÍPIOS DA LGPD

- Qual a finalidade do tratamento de dados pessoais?
- Todos os dados pessoais que a empresa irá coletar são necessários para atingir a finalidade para a qual eles serão utilizados?
- A finalidade do tratamento foi devidamente informada aos titulares dos dados de maneira clara e específica?
- O tratamento de dados é adequado às finalidades informadas aos titulares?
- O tratamento está em conformidade com o contexto e as expectativas dos titulares?
- A empresa está coletando dados desnecessários que não serão utilizados para uma finalidade específica?
- Existe uma forma menos invasiva de tratar esses dados coletando menor número de dados?
- Os titulares de dados possuem fácil acesso às informações sobre o tratamento de seus dados?
- A empresa oferece mecanismos adequados, acessíveis e transparentes para que os titulares possam consultar, solicitar a correção ou exclusão de seus dados?
- Quais medidas são adotadas pela empresa para garantir que os dados pessoais sejam exatos, atualizados e relevantes para a finalidade do tratamento?
- As operações de tratamento realizadas pela empresa possuem um potencial de restringir direitos ou liberdades dos titulares?
- A coleta dos dados foi realizada diretamente com os titulares ou eles foram compartilhados por outro controlador de dados?
- O uso de dados leva a decisões automatizadas que possam ser consideradas discriminatórias? Quais medidas são adotadas para evitar discriminações ilícitas ou abusivas contra os titulares?
- Onde, por quanto tempo e como os dados serão armazenados?
- Os titulares sabem quem são os agentes de tratamento responsáveis pela atividade? A identificação e contato do encarregado, ou do canal de atendimento, são fornecidas ao titular de maneira acessível?

- Os dados pessoais estão sendo compartilhados apenas com parceiros ou terceiros que seguem as diretrizes de proteção de dados? Existe contrato de tratamento de dados com os fornecedores e parceiros que compartilham esses dados?
- Quais as práticas de segurança da informação foram implementadas para garantir a segurança dos dados que a empresa está tratando? São realizadas auditorias e avaliações regulares para minimização de riscos e melhorias das práticas adotadas pela empresa?
- A empresa possui políticas claras e realiza treinamentos internos para garantir que todos os envolvidos entendam suas responsabilidades com relação à proteção de dados?
- A empresa possui mecanismos para identificar e corrigir violações de dados?
- A empresa está preparada para prestar contas à ANPD e aos titulares em caso de violações?
- A finalidade que a empresa inicialmente estabeleceu foi concluída? A empresa ainda precisa de todos os dados que foram coletados inicialmente?
- A finalidade inicial se alterou ao longo do tratamento?

Os princípios devem orientar todas as decisões ao longo do ciclo de vida dos dados pessoais na instituição, devendo ser analisados e reavaliados em todo o processo de adequação das operações de tratamento à LGPD.

5.2 BASES LEGAIS

As bases legais estão previstas no Art. 7° da LGPD para o tratamento de dados pessoais e no Art. 11 para o tratamento de dados pessoais sensíveis. Conforme o sistema estabelecido pela legislação, todo tratamento de dados deve estar respaldado por uma hipótese autorizativa, não existindo hierarquia entre as bases legais. Assim, a LGPD ampliou as possibilidades legais para o tratamento de dados, deixando claro que o consentimento não é a única justificativa apta a habilitar uma atividade de tratamento de dados pessoais.

Em conjunto com a aplicação dos princípios da LGPD, essas bases legais visam conferir legitimidade às operações de tratamento de dados.

BASES LEGAIS PARA **DADOS PESSOAIS** (ART. 7°, LGPD)	BASES LEGAIS PARA DADOS **PESSOAIS SENSÍVEIS** (ART. 11, LGPD)
Mediante o fornecimento de consentimento pelo titular	Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas
Para o cumprimento de obrigação legal ou regulatória pelo controlador	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	Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos
Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais	Realização de estudos, por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis
Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados **Para o 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)**	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)
Para a proteção da vida ou incolumidade física do titular ou de terceiro	Proteção da vida ou incolumidade física do titular ou de terceiro
Para a tutela da saúde, exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária	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 terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoas	**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. 9° da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.**
Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.	

Em relação aos dados pessoais sensíveis, a LGPD estabelece um regime de proteção mais rigoroso no Art. 11, devido ao maior risco de discriminação e à possibilidade de violação de direitos e garantias fundamentais. Esses dados incluem informações como “origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados relacionados à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural” (Art. 5º, II).

Por esse motivo, bases legais mais amplas, como o legítimo interesse, que são permitidas para dados não sensíveis, não se aplicam ao tratamento de dados sensíveis. Além disso, também se identifica uma diferença na redação da legislação para o consentimento, que deve ser específico, destacado e vinculado a finalidades claras.

A aplicação das bases legais para os agentes que operam no setor de saúde não é tarefa simples, existindo uma multiplicidade de hipóteses de aplicação de cada uma delas. O quadro abaixo apresenta exemplos não exaustivos conforme cada agente e possibilidades de tratamento sob determinada base legal:

Prestadores de serviços de saúde	Cumprimento de obrigação legal ou regulatória: manutenção de prontuário médico até 20 anos (Lei 13.783/2018). Proteção da vida ou incolumidade física: prestação de atendimento emergencial do titular ou terceiro. Tutela da saúde: compartilhamento de dados do paciente entre profissionais de saúde e prestadores de serviços da saúde, para assistência à saúde. Exercício regular de direitos: para defesa em processos judiciais e/ou administrativas. Legítimo Interesse: pesquisas de satisfação; marketing.
Operadoras de planos de saúde	Exercício regular de direitos: para defesa em processos judiciais em demandas envolvendo direito do consumidor ou trabalhista. Consentimento: gestão de saúde populacional. Prevenção à fraude e segurança do titular: uso de chaves eletrônicas em locais de acesso controlado, uso de biometria facial para acesso a aplicativo. Execução de contrato: coleta de dados do titular para adesão ao plano contratado. Cumprimento de obrigação legal ou regulatória: compartilhamento de dados com agentes da ANS conforme o padrão TISS (Resolução Normativa nº 501/2022). Legítimo Interesse: combate e prevenção à fraude securitária. Execução de contrato: coleta de dados para execução do contrato de compra e venda.
Fornecedores e distribuidores de produtos para saúde	Consentimento: respostas às pesquisas de quando envolverem dados pessoais sensíveis Cumprimento de obrigação legal ou regulatória: para rastreabilidade de dispositivos médicos em etiquetas, quando utilizados em procedimentos cirúrgicos (Resoluções RDC nº 59/2008, RDC 14/2011 e CFM nº 2.318/2022). Legítimo Interesse: combate e prevenção à fraude securitária.

Veja-se que a escolha da base legal apropriada para o tratamento de dados deve ser feita a partir da análise das particularidades da operação em questão, levando em conta a natureza dos dados envolvidos, a finalidade do processamento e a presença de obrigações legais ou regulatórias.

Diante das breves considerações sobre as hipóteses previstas na LGPD, os tópicos seguintes buscam analisar com mais detalhes as bases legais para tutela da saúde e o consentimento, ambas previstas para o tratamento de dados pessoais e dados pessoais sensíveis. Além delas, são analisadas as hipóteses do legítimo interesse, execução de contrato e cumprimento de obrigação legal ou regulatória pelo controlador, essas bases legais serão abordadas em detalhes a seguir.

5.2.1 LEGÍTIMO INTERESSE

O tratamento de dados para atendimento aos interesses legítimos do Controlador ou de Terceiro está previsto no âmbito do Art. 7º, IX da Lei, e será a base legal indicada quando não houver o tratamento de dados pessoais sensíveis e desde que os interesses e finalidades do controlador ou do terceiro não violem direitos e liberdades fundamentais do titular.

Para ser considerado legítimo, a ANPD indica que o interesse deve atender a três condições: “(i) compatibilidade com o ordenamento jurídico; (ii) lastro em uma situação concreta; e (iii) vinculação a finalidades legítimas, específicas e explícitas.”

Assim, recomenda-se a realização do teste de balanceamento para mapear e sopesar os interesses do controlador ou terceiro e os direitos e liberdades fundamentais dos titulares.

RECOMENDAÇÕES E PARÂMETROS DE INTERPRETAÇÃO CONFORME A ANPD PARA AVALIAÇÃO DO LEGÍTIMO INTERESSE

O tratamento de dados pessoais sempre deve ser restrito ao mínimo necessário para atender determinada finalidade pretendida.

O tratamento deve ser acompanhado da observância aos princípios da LGPD, com destaque às medidas práticas de transparência e minimização dos dados, garantindo-se que a informação seja adequada e compatível com a condição de criança e adolescente dos titulares (Art. 14, § 6º, da LGPD).

O tratamento de dados pessoais não deve ocorrer se, após a medida de ponderação no teste de balanceamento, concluir-se que as medidas de segurança e de mitigação de risco apropriadas não foram identificadas ou foram insuficientemente implementadas, ou identificou-se outras formas de tratamento alternativas e menos intrusivas aos direitos dos titulares, o que pode incluir o uso de outra base legal.

Se identificado o alto risco no tratamento de dados pessoais no caso concreto, deve-se elaborar o Relatório de Impacto à Proteção de Dados Pessoais.

ANPD. Guia Orientativo – Hipóteses legais de tratamento de dados pessoais – Legítimo Interesse. Fev/2024, p. 40. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf.

ANPD. Guia Orientativo – Hipóteses legais de tratamento de dados pessoais – Legítimo Interesse. Fev/2024, p. 40. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf.

Além disso, a LGPD define que a base legal do legítimo interesse somente pode ser utilizada nos casos de tratamento de dados para finalidades legítimas, podendo ser utilizada para atividades como apoio e promoção de atividades do controlador (art. 10, I, da LGPD); e proteção do exercício regular de direitos do titular ou prestação de serviços que o beneficiem (art. 10, II, da LGPD). A utilização desta base legal deve, contudo, observar os seguintes parâmetros:

respeitar as expectativas dos titulares (art. 10, II, da LGPD);

garantir os direitos e liberdades fundamentais dos titulares (art. 10, II, da LGPD);

utilizar apenas dados estritamente necessários para a finalidade pretendida (art. 10, § 1º, da LGPD);

adotar medidas que garantam a transparência no tratamento de dados (art. 10, § 2º, da LGPD); e

apresentar relatório de impacto à ANPD quando ela solicitar (art. 10, § 3º, da LGPD).

Para a análise dos elementos que permitam o uso adequado do legítimo interesse, a ANPD apresenta um modelo para realização do teste de balanceamento organizado em três etapas: i) finalidade, ii) necessidade e iii) balanceamento e salvaguardas Esse teste deve ser feito sempre que a base legal que justifica o tratado é o legítimo interesse, de acordo inclusive com o Guia de Legítimo Interesse da ANPD, que prevê que o “tratamento de dados com respaldo no legítimo interesse deve ser precedido de um teste de balanceamento”:

MODELO DE TESTE SIMPLIFICADO DO **TESTE DE BALANCEAMENTO DA ANPD**

Introdução

- Operação/tratamento:
- Data do teste:
- Atualizações:
- Preenchido por:
- Dados pessoais tratados:
- Finalidade do tratamento:
- Hipótese legal utilizada (legítimo interesse ou prevenção à fraude)

Parte I – Finalidade

- Natureza dos dados pessoais
- Qual a natureza dos dados pessoais?
- Existe tratamento de dados pessoais sensíveis? Em caso afirmativo, o tratamento não pode ser realizado com base na hipótese legal do legítimo interesse.
- Dados de crianças e adolescentes

Serão tratados dados de crianças e adolescentes?

Em caso positivo, o que foi considerado como melhor interesse dos titulares? Quais os critérios utilizados para a ponderação entre os interesses do controlador ou de terceiro e os direitos dos titulares? O tratamento gera riscos ou impactos desproporcionais e excessivos, considerando a condição da criança e do adolescente como sujeito de direitos?

O controlador possui uma relação prévia e direta com os titulares crianças e adolescentes? O tratamento visa assegurar a proteção de direitos e interesses dos titulares ou viabilizar a prestação de serviços que os beneficiem? Caso essas condições não estejam presentes, o controlador deve adotar cautela adicional, avaliando a existência de formas alternativas e menos invasivas para os titulares e, ainda, implementando as medidas de segurança e de mitigação de riscos adequadas à hipótese

- Interesse e finalidades legítimas

Qual benefício ou proveito resulta do tratamento de dados pessoais para o controlador ou terceiro?

O interesse é compatível com o ordenamento jurídico? Ou seja, o tratamento é compatível com princípios, normas jurídicas e direitos fundamentais? Aplicam-se ao caso e não se aplicam às hipóteses legais que vedam ou impeçam a realização do tratamento? O tratamento contraria, direta ou indiretamente, disposições legais ou princípios aplicáveis ao caso?

Qual a finalidade do tratamento? A finalidade é legítima, específica e explícita?

- Situação concreta

O interesse é baseado em uma situação clara, concreta e não especulativa?

Qual é essa situação concreta, de forma detalhada?

Qual o contexto em que é realizado o tratamento?

Parte II - Necessidade

- Tratamento e finalidade pretendida

O tratamento é necessário para atingir os interesses analisados no passo anterior?

É possível usar outros meios razoáveis para atingir a mesma finalidade de forma menos intrusiva para o titular?

O tratamento é proporcional e adequado para a finalidade descrita?

- Minimização

Estão sendo utilizados apenas os dados estritamente necessários para atingir à finalidade pretendida?

Existem formas menos intrusivas, menos onerosas ou com menores riscos ao titular que poderiam ser utilizadas para atingir a mesma finalidade?

Parte III – Balanceamento e salvaguardas

- Legítima expectativa

O tratamento dos dados pessoais para a finalidade pretendida é razoavelmente esperado pelos titulares, considerando o contexto em que é realizado?

A avaliação quanto à legítima expectativa deve levar em consideração, entre outros, os seguintes fatores relevantes:

Existe uma relação prévia do controlador com o titular?

Qual a fonte e a forma por meio das quais os dados foram coletados? Isto é, foram coletados diretamente do titular, de fontes públicas ou foram obtidos por meio de compartilhamento realizado por terceiros?

Qual o contexto e o período da coleta dos dados pessoais?

A finalidade original da coleta é compatível com o tratamento baseado no legítimo interesse?

- Riscos e impactos aos direitos e liberdades fundamentais

De que forma os titulares de dados pessoais serão impactados pelo tratamento?

Direitos e garantias fundamentais como liberdade de expressão, locomoção, não discriminação, intimidade, integridade física e moral podem ser afetados com o tratamento?

Quais são os riscos em potencial sobre os titulares?

Os direitos e liberdades fundamentais dos titulares prevalecem sobre os interesses do controlador ou de terceiro?

- Salvaguardas e mecanismos de opt-out e de oposição

Quais medidas são adotadas para mitigar os riscos identificados?

Quais medidas de transparência são adotadas? Serão disponibilizadas informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e respectivos agentes de tratamento?

Será disponibilizado canal de fácil acesso, por meio do qual os titulares podem exercer os direitos previstos na LGPD, em especial os de se descadastrar, de opor ao tratamento e de solicitar o término da operação e a eliminação de seus dados pessoais?

Conclusão

Analisar as respostas das Partes 1, 2 e 3 para concluir se pode ou não aplicar a hipótese legal do legítimo interesse.

É possível utilizar o legítimo interesse nesse tratamento de dados? Sim/Não

Comentários adicionais:

Data:

Local:

O exemplo do teste acima da ANPD pode ser adaptado conforme cada circunstância a depender da complexidade do tratamento ou outros fatores devidamente justificados pelo controlador. São exemplos de situações nas quais o legítimo interesse se aplica:

(a) pesquisa de satisfação enviada aos titulares com perguntas sobre determinado atendimento realizado, por exemplo, pode ser fundamentada no legítimo interesse, desde que realizado o devido teste de balanceamento;

(b) situações de marketing interno também podem ser fundamentadas no legítimo interesse, observando-se, sempre, os tipos de dados pessoais tratados.

Por fim, é importante ressaltar que o teste mencionado não fornece uma resposta definitiva sobre a legalidade do processamento. A decisão final cabe ao controlador, que deve avaliar cuidadosamente os benefícios e os riscos envolvidos, para proteção adequada dos direitos dos titulares.

5.2.2 CONSENTIMENTO

O consentimento, de acordo com o Art. 5º, XII, da LGPD, é a "manifestação livre, informada e inequívoca pela qual o titular concorda com o

manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Como base legal, além do Art. 7º, I, a LGPD prevê essa hipótese para o tratamento de dados pessoais sensíveis e acrescenta qualificações para que o consentimento seja considerado válido, ele deve ser específico e destacado (Art. 11, I).

Ademais, em relação ao tratamento de dados de crianças, e quando a justificativa selecionada para o tratamento for o consentimento, o Art. 14, § 1º, da LGPD prevê que ele deve ser específico, em destaque, e apresentado por pelo menos um dos pais ou pelo responsável legal.

É importante frisar que o consentimento enquanto base legal da LGPD se refere à autorização dada pelos titulares ou representantes legais para o tratamento de dados pessoais. Esse consentimento não se confunde com os casos de solicitação do consentimento para autorização de determinado procedimento de saúde como o Termo de Consentimento Livre e Esclarecido na assistência médica, definido pela Recomendação CFM nº 1/2016. Outro é o consentimento coletado para o compartilhamento de resultados devido à incidência da obrigação de sigilo médico.

Na prestação de serviços de saúde, é possível identificar disposições legais que orientam os controladores quanto ao uso do consentimento para determinados tratamentos de dados. A Resolução CFM nº 1.605/2000, por exemplo, define em seu Art. 1º que o médico não pode revelar o conteúdo do prontuário ou ficha médica sem o consentimento do paciente. Além disso, o Art. 54 da Resolução CFM nº 2.217/2018, que aprova o Código de Ética Médica, determina que os médicos não devem deixar de fornecer a outro médico informações sobre o quadro clínico de paciente, exceto quando vedado pelo paciente ou por seu representante legal.

A Nota Técnica da ANS nº 3/2019/GEPIN/DIRAD-DIDES/DIDES (Processo nº 33910.029786/2019-51) indica as seguintes orientações a respeito da gestão do consentimento por parte dos responsáveis pelo tratamento de dados:

"Não existe uma abordagem única para o teste de balanceamento. Em algumas circunstâncias, o teste pode ser breve ou simplificado, como nos casos em que é claramente identificada a existência de baixo impacto aos direitos dos titulares. Em outras situações, tal avaliação poderá Qdemandar maior detalhamento e robustez, como, por exemplo, no caso de uso de novas tecnologias baseadas em quantidades massivas de dados pessoais". ANPD. Guia Orientativo – Hipóteses legais de tratamento de dados pessoais – Legítimo Interesse. Fev/2024, p. 43. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf.

RECOMENDAÇÕES DA ANS PARA **GESTÃO DO CONSENTIMENTO**

- Identificação de todos os pontos de contato em que o consentimento dos dados é obtido.
- Identificação dos processos para os quais é necessário o consentimento.
- Identificação dos controladores de dados e processadores envolvidos com dados para os quais é necessário o consentimento.
- Revisão do gerenciamento de consentimento – se existente - no site e adaptação à LGPD.
- Revisão da gestão de consentimento existente em formulários em papel e adaptação à LGPD.
- Criação de repositório para gerenciamento de consentimento para garantir que o ônus da prova possa ser facilitado.

ANS. Nota Técnica nº 3/2019/GEPIN/DIRAD-DIDES/DIDES (Processo nº 33910.029786/2019-51), p. 13-14. Disponível em: https://sbac.org.br/wp-content/uploads/2019/12/Nota-Te%CC%81cnica-sobre-LGPD.pdf.

ACOMPANHAMENTO DE TRATAMENTOS DE **SAÚDE COM BASE NO CONSENTIMENTO**

Foi disponibilizado nas lojas de aplicativos de smartphone uma aplicação de saúde projetada para auxiliar os pacientes no acompanhamento detalhado de seus tratamentos médicos, com dados fornecidos pelo usuário e possibilidade de integração de dados de parceiros do setor da saúde.

Ao baixar o aplicativo, os usuários são imediatamente apresentados a uma mensagem com linguagem acessível, direta e explicativa, que serve para garantir o consentimento ativo para o compartilhamento de dados, principalmente em razão dos dados sensíveis, relativos à saúde.

O aplicativo conta com uma parte específica na qual o titular pode revogar o consentimento e isso foi arquitetado de forma que os tratamentos de dados são interrompidos. Nesse caso, o titular é apresentado às consequências disso, como maior tempo para agendar exames, desatualização das informações, entre outras consequências.

Esse aplicativo se destaca por sua abordagem centrada no usuário, priorizando a privacidade e o controle sobre dados de saúde. Ao basear todo o tratamento de dados no consentimento claro e informado, facilmente acessível e revogável, o aplicativo não apenas cumpre com as leis de proteção de dados, mas também estabelece um novo padrão em transparência e respeito à privacidade no setor de aplicativos de saúde.

CONSENTIMENTO VÁLIDO

Livre	o titular precisa ter efetivamente o poder de escolha sobre o tratamento de seus dados pessoais
Informado	ocorrer no contexto de que todas as informações necessárias para a decisão do titular sejam fornecidas, incluindo sobre quais são os efeitos do aceite ou recusa
Inequívoco	"uma manifestação de vontade clara e positiva do titular dos dados, não se admitindo a sua inferência ou a obtenção de forma tácita ou a partir de uma omissão do titular".
Específico	se referir a finalidades especificas, de modo a ser considerado nulo quando se verificar a indicação de autorizações genéricas para os responsáveis pelo tratamento (Art. 8º, §4º).

A LGPD apresenta outras orientações quanto ao uso do consentimento para o tratamento de dados pessoais. O consentimento deve obrigatoriamente ser fornecido por escrito ou outro meio válido que seja capaz de demonstrar a manifestação do titular (Art. 8º), cabendo ao controlador a responsabilidade de comprovar que o consentimento foi obtido legalmente, conforme a LGPD (Art. 8º, §2º). Se em meio escrito, é necessário o destaque desta cláusula com relação às demais (Art. 8º, §1º).

Caso o controlador precise compartilhar dados pessoais do titular com outros controladores, deve-se obter um novo consentimento específico exclusivamente para este fim, exceto nas hipóteses de dispensa do consentimento previstas em Lei (Art. 7º, §5º). Além disso, se forem alteradas as finalidades, forma, duração do tratamento, identificação do controlador ou as informações sobre o compartilhamento de dados, o titular deve ser informado e ele tem a possibilidade de revogar o seu consentimento se discordar das mudanças (Art. 8º, §6º).

RECOMENDAÇÕES AOS AGENTES DE TRATAMENTO PARA **OBTENÇÃO DO CONSENTIMENTO VÁLIDO SEGUNDO A LGPD**

- Disponibilize informações precisas, completas e compreensíveis ao titular, com destaque para:

Quais dados pessoais são tratados, identificando com precisão o grupo de pessoas envolvidas (por exemplo, é possível identificar entre "pacientes", "pacientes menores de 18 anos", "profissionais de saúde vinculados à instituição", dentre outros).

Informe qual a finalidade específica do tratamento dos dados pessoais.

Indique "se" e "com quem" há o compartilhamento de dados pessoais.

- Evite o uso de termos técnicos ou que possam ser confusos. Dê preferência ao uso de linguagem simples e acessível.
- Informe ao titular seus direitos, com destaque à possibilidade de revogação do consentimento, o meio para que isso ocorra e as possíveis consequências da escolha do titular.
- Estabeleça protocolos para registro do consentimento obtido do titular. Informações como data e hora da concessão ou revogação são bons exemplos sobre o que deve ser registrado.
- Permita que os titulares retirem o consentimento livremente a qualquer momento.
- Se for o caso, faça referência a outros documentos adotados pela instituição e meios de atendimento para resolução de dúvidas.
- Atualize os registros de consentimento sempre que houver alguma mudança relevante, como a ampliação de coleta de dados, compartilhamento com terceiros ou alteração da finalidade.
- Seja responsável e proativo, esteja preparado para demonstrar a sua conformidade com a LGPD quando for solicitado.
- Lembre-se de considerar a perspectiva do titular, e opte por, sempre que possível, adotar procedimentos que sejam de fácil compreensão.

ANPD. Guia Orientativo – Cookies e proteção de dados pessoais. Out/2022, p. 18-19. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf.

Nem sempre o consentimento será a base legal mais adequada, seja porque ele pode ser revogado a qualquer momento e comprometer a continuidade do tratamento, como também pelo risco de seu uso indiscriminado poder sobrecarregar o titular com muitos pedidos. Além disso, ressalta-se a dificuldade de realizar a gestão de todos os consentimentos obtidos pelo titular, razão pela qual recomenda-se que o Controlador tenha um processo interno específico para a sua gestão, no melhor cenário, por meio de uma plataforma específica.

Assim, os agentes de tratamento devem avaliar cuidadosamente quando da utilização do consentimento, uma vez que, quando for possível a utilização de outra base legal mais adequada, esta deve ser utilizada.

5.2.3 CUMPRIMENTO COM OBRIGAÇÕES LEGAIS E REGULATÓRIAS

Em razão da regulação setorial é comum que os agentes de tratamento do setor de saúde precisem compartilhar informações com o poder público para atender às obrigações legais e regulatórias, como normas definidas pela ANS (Agência Nacional de Saúde Suplementar), pela Anvisa (Agência Nacional de Vigilância Sanitária) e por conselhos profissionais, como o CFM (Conselho Federal de Medicina).

Nesse contexto, o cumprimento das obrigações de proteção de dados pessoais no setor de saúde vai além da simples conformidade legal. Ele se torna um fator determinante para a continuidade dos serviços, a eficiência e a lucratividade das atividades privadas, além de garantir o atendimento adequado à saúde dos cidadãos. A proteção de dados, portanto, se posiciona como um elemento estratégico para o setor.

Cabe destacar que a base legal para o cumprimento de obrigações regulatórias deve abranger não apenas leis, mas também decretos, resoluções, portarias, instruções normativas e demais normas emanadas dos poderes públicos.

EXEMPLOS DE OBRIGAÇÕES LEGAIS EM QUE HÁ **COMPARTILHAMENTO DE DADOS COM O PODER PÚBLICO**

- Envio periódico pelas operadoras de produtos à ANS de informações e estatísticas relativas às suas atividades, incluindo dados que permitam a identificação dos consumidores e de seus dependentes (Art. 20, Lei nº 9.656/1998).
- Notificação compulsória de determinas doenças, agravos e eventos de Saúde Pública, conforme previsto pelo Ministério da Saúde.
- Notificação de reação adversa à medicamento à Anvisa, através do sistema de notificação de eventos adversos de medicamentos “VigiMed”.
- Emissão de certidão de nascimento em estabelecimentos de saúde que realizem o parto (Resolução CNJ nº 13/2010).
- Rastreabilidade de dispositivos médicos, como implantes ortopédicos (RDC nº Anvisa 59/2008) e materiais implantáveis (RDC Anvisa nº 14/2011).
- Internação psiquiátrica involuntária devem ser comunicadas em até setenta e duas horas ao Ministério Público Estadual (Art. 8º, §1º, Lei nº 10.216/2001).
- Notificação ao Ministério da Saúde de todos os resultados de testes diagnóstico para SARS-CoV-2 realizados por laboratórios da rede pública, rede privada, universitários e quaisquer outros, em todo território nacional (Portaria MS nº 1.792/2020).
- Envio de resultados de teste de Covid-19 por laboratórios da rede pública, rede privada, universitários e quaisquer outros, em todo território nacional pela RNDS (Portaria GM/MS nº 1.046/2021).
- Notificação à Central de Notificação Captação e Distribuição de Órgãos e Tecidos (CNCDO) em casos falência da atividade cerebral irreversível e a família concorda em doar os órgãos do parente (Portaria MS nº 2.600/2009).

Lista unificada atualizado em 19/02/2024, disponível em: https://www.gov.br/saude/pt-br/composicao/svsa/notificacao-compulsoria/lista-nacional-de-notificacao-compulsoria-de-doencas-agravos-e-eventos-de-saude-publica.

Formulário atualizado em 1º/11/2022, disponível em: https://www.gov.br/anvisa/pt-br/assuntos/noticias-anvisa/2021/anvisa-disponibiliza-novo-formulario-para-notificacao-de-eventos-adversos.

Importante destacar que a previsão de obrigações legais que exigem o compartilhamento de dados com o poder público não exime as instituições de realizarem o tratamento dados pessoais respeitando as condições de legitimidade da LGPD e obrigações nela prevista, de modo que os agentes de tratamento devem garantir que o risco da operação de tratamento seja devidamente e proporcionalmente endereçado.

Nesse sentido, além da avaliação da base legal, é necessário especial atenção com o cumprimento com os princípios que regulam o tratamento, com destaque ao da minimização, para que os dados tratados sejam apenas os necessários e adequados à finalidade específico, e sejam mantidos somente durante o período que forem pertinentes e limitados aos objetivos do tratamento. Assim, recomendamos que as seguintes medidas sejam adotadas na adoção da referida base legal:

BOAS PRÁTICAS PARA A PROTEÇÃO DE DADOS AO CUMPRIR OBRIGAÇÕES LEGAIS E REGULATÓRIAS

- Identifique qual hipótese legal respalda a operação de tratamento de dados e, se possível, recorra ao jurídico para obter apoio na interpretação de obrigações legais e regulatórias.
- Mapeie as normas que ensejam o compartilhamento de dados pessoais e estabeleça protocolos seguros para realização desse compartilhamento.
- Em caso de pedido de compartilhamento de dados, avalie se é possível adotar medidas de minimização do impacto do compartilhamento de dados, como a pseudonimização e anonimização das informações, e ocultamento de dados pessoais desnecessários para a finalidade pretendida.
- Mantenha atualizado o registro das operações de compartilhamento de dados, apontando quais dados foram exigidos, o prazo dado para cumprimento da solicitação (quando aplicável), medidas de segurança e minimização adotadas, com qual autoridade o dado foi compartilhado e qual o respaldo legal.
- Adote medidas técnicas e administrativas robustas para proteger as atividades que envolvem os dados (como os processos de coleta, armazenamento e compartilhamento) contra ameaças, como acessos não autorizados, perdas e danos.

5.2.4 EXECUÇÃO DE CONTRATO

É comum que o processamento de dadosCaso seja necessário o compartilhamento de dados pessoais com autoridades competentes, como para atender a determinações judiciais e cooperar com autoridades policiais, as organizações podem estabelecer fluxos internos para avaliação das solicitações, o que pode envolver a criação de um canal de comunicação oficial específico para o recebimento e direcionamento das solicitações, e o treinamento para que os funcionários encaminhem as demandas aos setores responsáveis.

Com auxílio do encarregado, deve-se buscar garantir que o compartilhamento seja apenas sobre os dados estritamente necessários para atender à solicitação, e devem ser adotadas medidas de segurança, técnicas e organizacionais, para proteção dos dados pessoais durante todo o processo de compartilhamento.

Dessa forma, as medidas a serem adotadas pelas instituições podem auxiliá-las a atenderem de forma específica as exigências legais em tempo hábil e de maneira segura, conforme as determinações da LGPD.

pessoais seja necessário para que os contratos firmados pelo próprio titular sejam cumpridos ou mesmo para atender alguma condição pré-contratual. A LGPD reconhece essa realidade e, por isso, prevê a execução contratual como uma das hipóteses que subsidia o tratamento de dados (Art. 7º, V). Em caso de dados pessoais sensíveis, a lei autoriza o tratamento de dados para o exercício regular de direitos previstos em contrato (Art. 11, II, “d”).

O contrato previsto na LGPD não precisa ser um documento formal assinado, ou mesmo escrito. Qualquer contrato reconhecido pela lei civil é suficiente para que justifique o tratamento de dados. Ainda, é possível usar a base legal prevista no Art. 7º, V mesmo em casos os quais ainda não há contrato firmado, mas que o tratamento seja necessário para a negociação dos termos na fase pré-contratual. Nesses casos, o titular deve pedir que o tratamento ocorra, de forma a não ser possível usar essa base para quando a empresa inicia o processo de negociação contratual por iniciativa própria, sem provocação do titular.

ENVIO DE COTAÇÃO PELAS OPERADORAS DE PLANOS DE SAÚDE

Uma operadora de plano de saúde está realizando campanha publicitária para alcançar novos clientes. Como resultado da campanha, a operadora recebe inúmeros pedidos de cotação enviados pelos próprios titulares. Essa operadora pode se valer da base legal de procedimentos preliminares de execução do contrato para coletar dados necessários para elaborar a cotação, como nome, idade e endereço.

COLETA DE DADOS PARA EXECUÇÃO DE CONTRATOS DE SERVIÇOS DE SAÚDE

Um titular visitou um laboratório para fazer seus exames de rotina. Para tanto, o titular compartilhou com o laboratório seu nome, documento de identificação, carteirinha do plano de saúde, pedido médico e seu e-mail para que fosse possível realizar os exames solicitados e para que o resultado fosse enviado por correio eletrônico para o titular. O contrato firmado entre o laboratório e o titular tinha como objetivo a realização do exame e posterior acesso aos resultados. Por isso, apesar do laboratório conhecer e-mail do titular, ele não pode ser usado para finalidades que não estejam amparadas pelo escopo. Se o laboratório quisesse enviar campanhas publicitárias para o e-mail do titular, por exemplo, essa atividade não estaria autorizada pela base legal da execução de contrato e outras bases legais deveriam ser analisadas para verificar a viabilidade do tratamento.

Essa base legal se aplica a cenários em que a empresa do setor de saúde trate dados pessoais do titular para que as obrigações firmadas nos contratos sejam cumpridas, como a prestação de um serviço médico, a aquisição de um produto para saúde, ou o processamento do pagamento como contrapartida.

Ainda, a execução de contrato pode ser utilizada para justificar o tratamento de dados necessário para contraprestação do contrato firmado. Ou seja, a base legal justifica o tratamento de dados de interesse de ambas as partes do contrato. O tratamento deve ser orientado por um esforço de minimização e adequação do tratamento, de forma que apenas os dados necessários para a execução do contrato sejam tratados e da forma menos intrusiva possível para o titular.

TRATAMENTO DE DADOS NO FORNECIMENTO DE PRODUTOS PARA SAÚDE

Durante processo de compra de um produto para saúde, o fornecedor solicita alguns dados da pessoa que adquire o produto. Em regra, o produto é adquirido por pessoa jurídica, sem o tratamento de dado pessoal.

Quando a compra é realizada por pessoa física, é possível que o fornecedor colete dados de pagamento do titular, por exemplo dados do cartão de crédito, como número do cartão, data de expiração e código CVV. Esse dado é fundamental para garantir que a contraprestação, uma obrigação da parte que forma o contrato, será respeitada. Em momento posterior, a empresa fornecedora inicia projeto de análise de qual bandeira de cartão é mais utilizada por seus clientes a fim de formular melhorias para suas condições de pagamento e retoma o tratamento de dados do número do cartão dos titulares, informações que foram coletadas para a execução de contrato de compra dos produtos. O fornecedor percebe que não poderá usar essa base legal para tratar esses dados e passa a avaliar o uso de outras hipóteses.

Importante reforçar que os princípios devem ser criteriosamente considerados no tratamento de dados. Por exemplo, ainda que a base legal utilizada seja a da "execução de contrato", os dados tratados para o seu cumprimento devem atender, por exemplo, aos princípios da necessidade e finalidade (Art. 6, I e III, LGPD). Da mesma forma, ainda que um dado pessoal seja tratado com o consentimento de seu titular, o tratamento não pode ser realizado para fins discriminatórios, ilícitos ou abusivos (Art. 6, IX, LGPD).

CHECKLIST PARA TRATAMENTO DE DADOS COM BASE NA EXECUÇÃO DE CONTRATO

- Existe um contrato válido entre a empresa e o titular dos dados;
- O contrato não é nulo, anulável ou inexequível de outra forma;
- Há uma ligação direta e específica entre o processamento e a finalidade do contrato;
- O processamento não é apenas útil ou prática comercial padrão, mas essencial;
- O titular dos dados esperaria razoavelmente esse processamento como parte do contrato;
- A empresa está processando apenas os dados necessários para o contrato;
- A empresa documentou sua decisão de usar o contrato como base legal;
- A empresa pode justificar essa escolha se for questionado;
- A empresa implementou processos para lidar com os direitos do titular dos dados (por exemplo, acesso, retificação, restrição).

FUJIMOTO, Mônica Tiemy. Comentário ao Art. 7º, VIII, da LGPD: no prelo.

5.2.5 TUTELA DA SAÚDE

A base legal da tutela da saúde é prevista no Art. 7º, VIII, e 11, II, f, da LGPD. Apesar de incisos diferentes, eles possuem a mesma redação: "tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária".

Assim, entende-se que para melhor interpretação, é necessária a adoção de parâmetros interpretativos acerca da interpretação de quatro partes:

"tutela de saúde",

"exclusivamente",

"em procedimento realizado por", e

"profissionais de saúde, serviços de saúde ou autoridade sanitária".

A "tutela da saúde" engloba as atividades de tratamento de dados pessoais sensíveis ou não que tenham como finalidade a proteção da saúde da pessoa, seja física ou mental. Ao mesmo tempo que a existência dessa base legal é uma garantia de segurança jurídica para o setor da saúde, a sua aplicação ainda gera bastante incerteza, especialmente por conta da inclusão do termo "exclusivamente". Isso porque a exclusividade apresentada na Lei indica para uma interpretação restritiva da sua aplicação que é incompatível com as necessidades do setor.

Já os termos "em procedimento realizado por", e "profissionais de saúde, serviços de saúde ou autoridade sanitária" levam à interpretação de que não é qualquer pessoa que está autorizada a tratar dados com base na tutela da saúde. Para que isso seja possível, os agentes com qualificações específicas devem realizar procedimentos de saúde. O agente deve ser um profissional de saúde, ou um serviço de saúde ou uma autoridade sanitária.

Cumpre destacar que, inicialmente, o texto legislativo apenas indicava "profissionais de saúde" e "autoridades sanitárias". Contudo, a Lei nº 13.853/2019 introduziu o termo "serviços de saúde" para que fossem contemplados outros agentes privados.

Condições para uso da base legal de tutela da saúde

Atividade de tratamento realizada para tutelar à saúde do titular ou de terceiros.

Atividade realizada por: Profissionais de saúde; Serviços de saúde; ou Autoridade sanitária.

Ressalta-se que o Art. 11 da LGPD fornece mais orientações que reforçam a necessidade de atenção quando da aplicação desta base legal. Dentre essas determinações estão:

A autoridade nacional pode proibir ou regular a comunicação e o compartilhamento de dados pessoais sensíveis entre controladores que buscam vantagem econômica, após consulta aos órgãos setoriais competentes (Art. 11, §3º).

A comunicação ou compartilhamento de dados sensíveis de saúde entre controladores com o objetivo de obter vantagem econômica é proibido. Esse tratamento só é permitido para a prestação de serviços de saúde, assistência farmacêutica,

assistência à saúde e diagnóstica, em benefício do titular, e para permitir transações financeiras e administrativas associadas, e ou a portabilidade de dados a pedido do titular (Art. 11, §4º).

Operadoras de planos de saúde não podem utilizar dados de saúde para selecionar riscos na contratação ou exclusão de beneficiários (Art. 11, §5º).

Insta destacar que a ANS, por meio da Nota Técnica nº 3/2019/GEPIN/DIRAD-DIDES/DIDES, no processo nº 33910.029786/2019-51, afirma que a base legal de tutela da saúde autoriza a "utilização de informações de saúde por gestores de sistemas de saúde públicos ou privados para a condução de programas de promoção de saúde e de prevenção de doenças, bem como para o direcionamento dos pacientes para prestadores mais adequados para seus quadros".

Para a ANS, operadoras de planos de saúde são gestores privados da saúde. Como consequência, a agência entende que as operadoras poderiam tratar informações de saúde para promover a saúde, prevenir doenças ou direcionar pacientes para prestadores adequados para seus quadros.

Destaca-se que o tratamento de dados pessoais, especialmente os dados sensíveis, requer postura ativa e preventiva dos agentes de tratamento. Por isso, o operador deve adotar as melhores práticas para estar em conformidade com a LGPD e realizar o tratamento de forma transparente, menos intrusiva possível e respeitando as os direitos dos titulares e os princípios da LGPD. Isso significa que o tratamento deve ser compatível com a finalidade informada ao titular e esse tratamento deve ter como objeto apenas os dados estritamente necessários e não excessivos para atingir uma finalidade específica e legítima.

Nesse sentido, é altamente recomendável que os agentes a seu critério, avaliem o uso de ferramentas de pseudonomização ou anonimização dos dados a fim de reduzir os riscos do tratamento. Ainda, o tratamento deve ser conhecido pelo titular e ele deve ter ferramentas para a transparência, o livre acesso e a garantia da qualidade dos dados.

Veja-se que a interpretação da base legal para tutela da saúde requer uma maior cautela por conta de seu grande potencial lesivo do tema "saúde" para os titulares dos dados pessoais. Dessa forma, o agente responsável pelo tratamento deve adotar medidas robustas de governança e segurança dos dados, especialmente dos dados pessoais sensíveis, garantindo que eles não serão tratados para fins discriminatórios ilícitos ou abusivos.

PARTE II

MELHORES PRÁTICAS PARA O SETOR DE SAÚDE

6. ESPECIFICIDADES DO SETOR DE SAÚDE

Especificidades do setor de saúde

Conforme mencionado no tópico III, o setor de saúde realiza uma grande variedade de operações de tratamentos de dados pessoais que são essenciais para inúmeras atividades. Esses dados são indispensáveis tanto para operações básicas, como processamento de pagamentos, faturamento, cobrança e emissão de notas fiscais, quanto para o desenvolvimento de novas tecnologias. Veja-se que inovações como telessaúde e monitoramento remoto facilitam o atendimento ao paciente, reduzindo o tempo de espera e deslocamento, além de tornar o acesso aos serviços de saúde mais conveniente e adaptado às necessidades individuais.

O uso dessas tecnologias também melhora a eficiência operacional, automatizando processos administrativos, como agendamento de consultas, realização de cobranças e gestão de estoque. Isso sem contar a contratação de serviços essenciais, como provedores de hospedagem de dados, plataformas de prontuário eletrônico, meios de pagamento e logística de transporte de documentos e materiais biológicos.

Assim, a amplitude e a diversidade dos dados tratados no setor trazem desafios significativos, exigindo que o setor equilibre os benefícios da inovação com os riscos de um tratamento inadequado.

Nesta seção, serão abordadas algumas operações no setor de saúde que exigem maior atenção, como o uso de prontuário eletrônico, telessaúde, relações com terceiros, prevenção e promoção da saúde, realização de auditorias e a utilização de ferramentas de identificação.

6.1 PRONTUÁRIO ELETRÔNICO

O prontuário eletrônico do paciente (PEP) é um "repositório de informações mantidas de forma eletrônica, ao longo da vida de um indivíduo". Diferente do prontuário digitalizado, que é redigido manualmente em papel e depois pode ser digitalizado, o prontuário eletrônico normalmente é criado e acessado pelo profissional de saúde através de um software médico. Assim, o PEP auxilia no armazenamento, organização e gerenciamento das informações de saúde dos pacientes de forma estruturada e segura.

Além disso, com o PEP é possível o uso de ferramentas de pesquisa, o que facilita a localização e cruzamento de informações com agilidade para benefício do cuidado do paciente. As informações que podem estar disponíveis neste documento são:

MINISTÉRIO DA SAÚDE. Prontuário eletrônico. Disponível em: https://www.gov.br/saude/pt-br/composicao/saps/informatiza-aps/prontuario-eletronico.

CONSENTIMENTO VÁLIDO

Dados de identificação do paciente	**Nome, data de nascimento, código do plano de saúde ou outra credencial.**
Dados de saúde	**Registro e avaliação de anamnese, exame objetivo e variáveis clínicas, prescrição de medicamentos ou outros métodos terapêuticos; tratamentos anteriores e em andamento; alergias; solicitação e resultado de exames e outros métodos diagnósticos complementares; consultas anteriores com outros profissionais; emissão de atestados e demais documentos clínicos.**
Dados de identificação do profissional de saúde responsável pelo atendimento do paciente	**Nome, registro profissional.**

O PEP é comumente utilizado na prática de telessaúde e, caso seja emitido à distância relatório, atestado ou prescrição médica, deve constar de forma obrigatória no prontuário as seguintes informações, conforme estipulado pelo Art. 13 da Resolução CFM nº 2.314/2022:

INFORMAÇÕES OBRIGATÓRIAS QUE DEVEM CONSTAR NO **PRONTUÁRIO EM CASO DE TELESSAÚDE**

- Identificação do médico, incluindo nome, CRM, endereço profissional.
- Identificação e dados do paciente (endereço e local informado do atendimento).
- Registro de data e hora.
- Assinatura com certificação digital do médico no padrão ICP-Brasil ou outro padrão legalmente aceito.
- Informação de que foi emitido em modalidade de telessaúde.

Informações obtidas a partir de: MINISTÉRIO DA SAÚDE. Prontuário eletrônico. Disponível em: https://www.gov.br/saude/pt-br/composicao/saps/informatiza-aps/prontuario-eletronico.

Identificação do médico, incluindo nome, CRM, endereço profissional.

Identificação e dados do paciente (endereço e local informado do atendimento).

Registro de data e hora.

Assinatura com certificação digital do médico no padrão ICP-Brasil ou outro padrão legalmente aceito.

Informação de que foi emitido em modalidade de telessaúde.

Informações obtidas a partir de: MINISTÉRIO DA SAÚDE. Prontuário eletrônico. Disponível em: https://www.gov.br/saude/pt-br/composicao/saps/informatiza-aps/prontuario-eletronico.

O armazenamento das informações exige cuidados especiais para garantir a privacidade e a segurança das informações pessoais. O Art. 4º da Lei nº 13.787/2018 dispõe explicitamente que a proteção exigida sobre os documentos digitais requer medidas contra o acesso, uso, alteração, reprodução e destruição não autorizadas.

No caso de tratamento de dados de crianças e adolescentes, deve-se adotar maior cautela diante da incidência de outras proteções jurídicas, como aquelas previstas no Estatuto da Criança e do Adolescente (ECA). Assim, todas as atividades devem ocorrer visando o seu melhor interesse, como determina a LGPD em seu Art. 14.

Além disso, é recomendável que os responsáveis pelo tratamento informem de maneira clara, acessível e de fácil compreensão as informações sobre o tratamento dos dados, aos pais ou aos responsáveis legais, para que a obtenção do consentimento específico de fato seja livre, esclarecido e em destaque. Nesse sentido, uma salvaguarda importante que cabe às instituições é a adoção de medidas seguras e proporcionais para a comprovação da identificação e do vínculo do responsável legal.

A respeito das demais bases legais, o Enunciado CD/ANPD nº 1/2023 indica que todas as hipóteses previstas nos artigos 7º e 11 da LGPD podem ser utilizadas desde que o princípio do melhor interesse desse grupo seja não apenas observado, como prevalecente.

Cabe considerar que a ANPD considera dentre os requisitos de elaboração do Relatório de Impacto à Privacidade de Dados (RIPD) o grupo de idosos, caso ocorra o tratamento de dados pessoais sensíveis, como vulnerável junto ao de crianças e adolescentes como um dos critérios específicos de avaliação do tratamento de alto risco (Art. 4º, II, d, da Resolução CD ANPD nº 2/2022). Para este perfil, também é recomendável o uso de comunicação compreensível, evitando termos técnicos ou complicados.

Na definição do período de armazenamento dos dados, deve-se observar o prazo de 20 (vinte) anos estipulados pela Lei nº 13.787/2018 (Art. 6º) e a Resolução CFM nº 1.821/2007 (Art. 8º), que abrangem as informações de saúde digitalizadas e o uso de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.

Nesse sentido, são recomendadas as seguintes boas práticas para proteção de dados pessoais em PEPs:

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente."O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei." Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf.

BOAS PRÁTICAS PARA PROTEÇÃO DE DADOS PESSOAIS EM PRONTUÁRIOS ELETRÔNICOS

- Quando possível, utilize medidas de pseudonimização e anonimização dos dados pessoais.
- Minimize a coleta de dados com a coleta apenas dos dados estritamente necessários para a finalidade pretendida, evitando o tratamento de dados desnecessários ou excessivos.
- Informe os titulares de dados de maneira clara e acessível sobre como seus dados serão utilizados, com quem serão compartilhados, e por quanto tempo serão armazenados.
- Crie e mantenha atualizados a política de privacidade e os termos de uso que descrevam claramente como os dados são armazenados, processados e protegidos.
- Mantenha o registro do tratamento de dados pessoais e avalie a necessidade de elaboração de outros documentos, como o Relatório de Impacto à Privacidade de Dados (RIPD).
- Adote procedimentos para segurança dos dados, como, por exemplo, protocolo HTTPs, criptografia e acesso segmentado de acordo com as funções de cada um no local de atendimento ao paciente.
- Realize backups de segurança periodicamente, para garantir que os dados possam ser recuperados em caso de perda e demais incidentes.
- Opte pelo uso de equipamentos, como computadores, profissionais e evite o uso de dispositivos pessoais ou de terceiros para acesso aos documentos.
- Faça uso de sistemas de proteção dos equipamentos para acesso ao prontuário, com instalação de programas de antivírus recomendados.
- Utilize redes de acesso à internet seguras e evite acesso à rede Wi-Fi públicas ou desconhecidas.
- Atente-se aos requisitos de certificação digital e ao nível de segurança exigidos para o uso do prontuário digital. O Conselho Federal de Medicina exige o Nível de garantia de segurança 2 (NGS2), estabelecidos no Manual de Certificação para Sistemas de Registro Eletrônico e em Saúde (Resolução CFM nº 1.821/2007). Assim, os arquivos a serem utilizados devem garantir a autenticidade, confidencialidade e integridade dos dados, através do uso da certificação digital, assinatura digital, e criptografia, por exemplo.
- Providencie o treinamento técnico para o uso do software, com orientações para promoção da proteção de dados em seu local de trabalho.
- Realize auditorias internas para verificar se os procedimentos de armazenamento de documentos estão sendo seguidos corretamente.
- Os agentes de tratamento também precisam se atentar ao processo de eliminação dos documentos, pois é necessário resguardar a "intimidade do paciente e o sigilo e a confidencialidade das informações" (Art. 6º, §3º, da Lei nº 13.787/2018). No caso de documentos digitalizados, recomenda-se a avaliação sobre a exclusão das versões originais físicas, o que pode incluir a trituração dos arquivos e outros meios que protejam a privacidade dos pacientes.

6.2 TELESSAÚDE

A telessaúde – também chamada de telemedicina - é um exemplo claro de como os avanços tecnológicos têm transformado a área da saúde. Esses avanços permitiram que a prestação de cuidados médicos superasse as barreiras geográficas e temporais, proporcionando maior acessibilidade e eficiência nos serviços de saúde. De acordo com a definição legal, a telessaúde é a "prestação de serviços de saúde a distância, por meio da utilização das tecnologias da informação e da comunicação", que deve envolver "a transmissão segura de dados e informações de saúde, por meio de textos, de sons, de imagens ou outras formas adequadas" (Art. 26-B, da Lei nº 8.080/1990, atualizada pela Lei nº 14.510/2022 para dispor sobre a telessaúde).

Assim, a telessaúde pode ser compreendida como uma forma ampla de ações desenvolvidas através tecnologias de informação e comunicação no setor de saúde, porque abrange a "prestação remota de serviços relacionados a todas as profissões da área da saúde regulamentadas pelos órgãos competentes do Poder Executivo federal" (Art. 26-A, da Lei nº 8.080/1990).

Como exemplos de tratamento de dados pessoais, é possível indicar o uso de informações dos profissionais de saúde para cadastro e acesso a plataformas de telemedicina, para os quais podem ser exigidos o nome, e-mail, telefone, e demais dados exigidos pelo serviço utilizado.

Para todos os usos de modalidades de telessaúde devem ser observados os seguintes princípios em todas as etapas de uso:

PRINCÍPIOS PARA USO DA TELESSAÚDE NO BRASIL

Autonomia do profissional de saúde	O profissional de saúde tem autonomia para escolher as ferramentas e tecnologias que julgar mais adequadas para prestar o atendimento, dentro dos limites da legislação e da ética médica. Nesse mesmo sentido, o Art. 26-C da Lei nº 8.080/1990 assegura aos profissionais a "liberdade e a completa independência de decidir sobre a utilização ou não da telessaúde", e podem, sempre que entenderem necessário, optar pelo atendimento presencial (Art. 26-A, I, da Lei nº 8.080/1990).
Consentimento livre e informado do paciente	O paciente deve ser devidamente informado sobre os procedimentos, benefícios e riscos da telessaúde, e consentir livremente em participar (Art. 26-A, II, da Lei nº 8.080/1990).
Direito de recusa ao atendimento na modalidade telessaúde	É direito do paciente de optar pelo atendimento presencial a qualquer momento, sem prejuízo à continuidade do cuidado (Art. 26-A, III, da Lei nº 8.080/1990).
Dignidade e valorização do profissional de saúde	Envolve os elementos de exercício profissional, como condições adequadas de trabalho (Art. 26-A, IV, da Lei nº 8.080/1990)
Assistência segura e com qualidade ao paciente	Garantia das mesmas qualidade e segurança do atendimento presencial, com o uso de tecnologias confiáveis e a adoção de protocolos adequados (Art. 26-A, V, da Lei nº 8.080/1990).
Confidencialidade dos dados	Dados devem ser tratados com segurança e protegidos contra acessos não autorizados (Art. 26-A, VI, da Lei nº 8.080/1990).
Promoção da universalização do acesso dos brasileiros às ações e aos serviços de saúde	Ações de desenvolvimento da telessaúde devem poder contribuir para ampliação do acesso aos serviços de saúde, especialmente para populações em áreas remotas ou com dificuldades de locomoção (Art. 26-A, VII, da Lei nº 8.080/1990).
Estrita observância das atribuições legais de cada profissão	Respeito às normas específicas que regem cada área de atuação. O Art. 26-D da Lei nº 8.080/1990 também indica que cabe aos conselhos federais de fiscalização do exercício profissional a normatização ética sobre o uso da telessaúde, semelhante às modalidades presenciais no que não for conflitante com a Lei nº 8.080/1990 e determinações sobre telessaúde (Art. 26-A, VIII, da Lei nº 8.080/1990).
Responsabilidade digital	O uso da telessaúde deve ser realizado de forma responsável e ética, seguindo as normas e regulamentações vigentes (Art. 26-A, XI, da Lei nº 8.080/1990).

Além disso, para o uso da telessaúde o Art. 26-G, da Lei nº 8.080/1990, determina a observância de que a práticas só devem ser realizadas apenas se houver o consentimento livre e esclarecido do paciente, ou de seu representante legal, e sob responsabilidade do profissional de saúde (Art. 26-G, I), bem como deve ocorrer a garantia do cumprimento de leis aplicáveis ao tema, dispostas no Art. 26-G, II: Marco Civil da Internet (Lei nº 12.965/2014), Lei do Ato Médico (Lei nº 12.842/2013), LGPD (Lei nº 13.709/218), Código de Defesa do Consumidor (Lei nº 8.078/1990) e, quando aplicável, a Lei do Prontuário Eletrônico (Lei nº 13.787/2018).

O consentimento livre e esclarecido acima não é o mesmo que a LGPD demanda, o uso de dados derivados de telessaúde podem ser justificados por outras hipóteses legais de tratamento de dados. Ademais, é possível o tratamento de outros dados pessoais de pacientes, como informações financeiras para pagamento sejam registradas para o serviço ou com o profissional que oferte a telessaúde.

Por isso, as organizações devem avaliar cuidadosamente as hipóteses de aplicação da telessaúde e, quando do uso de dados pessoais, considerar previamente e adequar as atividades conformes as condições de legitimidade para o tratamento. De toda forma, os princípios da necessidade, adequação e finalidade devem orientar a coleta mínima dos dados exigidos para o alcance do objetivo da atividade, e os titulares devem ser informados sobre seus direitos de forma ampla, clara e acessível.

Recomenda-se que antes da contratação ou desenvolvimento de serviços para telessaúde, os responsáveis se certifiquem que as plataformas garantam a segurança das informações e estejam em conformidade com a LGPD. Neste sentido, é importante considerar a existência e qualidade de documentos como, por exemplo, a Política de Privacidade, Política de Cookies, Identificação dos Agentes de Tratamento e Encarregado. Em algumas hipóteses, pode ser relevante a elaboração do Relatório de Impacto à Proteção de Dados (RIPD) e, para todas as atividades, orienta-se a documentação e mapeamento do tratamento de dados para promoção da governança de dados.

RECOMENDAÇÕES PARA A SEGURANÇA DA INFORMAÇÃO

- Armazene as informações do teleatendimento em um local seguro e de acordo com as normas de confidencialidade de dados de saúde.
- É recomendável a realização de backups de forma periódica.
- Utilize senhas fortes e as atualize periodicamente (a cada seis meses, por exemplo).
- Utilize redes de acesso à internet confiáveis e mantenha seus dispositivos e aplicativos atualizados.
- Utilize sistemas de antivírus e proteção para seus dispositivos.
- A emissão de documentos médicos através de TDICs deve ser por meio de assinatura digital, com Nível de Garantia de Segurança 2 (NGS2) (Art. 4º, da Resolução CFM nº 2.299/2021).
- As informações do prontuário, incluindo assinaturas, devem seguir os requisitos do Nível de Garantia de Segurança 2 (NGS2) no padrão da infraestrutura de Chaves Públicas Brasileira (ICP--Brasil), ou outro padrão legalmente aceito (Art. 3º, §2º, da Resolução CFM nº 2.134/2022).
- Garanta que os documentos e tecnologias utilizadas permitam a interoperabilidade das informações, de modo que as informações estejam armazenadas e comunicáveis entre si de forma segura.
- Desenvolva procedimentos de revisão e auditoria periódicos para segurança dos sistemas e das informações.

Além disso, é necessário que todas as pessoas da equipe sejam treinadas e capacitadas para exercerem determinadas funções atinentes à telessaúde. Medidas como a restrição de o acesso a documentos e informações de acordo com a respectiva função são recomendadas, além da assinatura de Termos de Confidencialidade.

Outro conceito relevante ao tema se refere à telessaúde, que envolve o atendimento clínico do paciente. De acordo com o Art. 1º da Resolução CFM nº 2.314/2022, a telessaúde é o exercício da medicina através do uso de "Tecnologias Digitais, de Informação e de Comunicação (TDICs), para fins de assistência, educação, pesquisa, prevenção de doenças e lesões, gestão e promoção de saúde".

Os avanços tecnológicos no uso da telessaúde exigem cuidados especiais na implementação de medidas de proteção de dados. Conforme o Art. 5º da Resolução CFM nº 2.314/2022, é possível a prática das seguintes modalidades no território brasileiro:

MODALIDADES DO EXERCÍCIO DA TELESSAÚDE (RESOLUÇÃO CFM Nº 2.314/2022)

Teleconsulta	Consulta médica não presencial, mediada por TDICs, com médico e paciente localizados em diferentes espaços.
Teleinterconsulta	Troca de informações e opiniões entre médicos, com auxílio de TDICs, com ou sem a presença do paciente, para auxílio diagnóstico ou terapêutico, clínico ou cirúrgico.
Telediagnóstico	Ato médico a distância, geográfica e/ou temporal, com a transmissão de gráficos, imagens e dados para emissão de laudo ou parecer por médico com registro de qualificação de especialista (RQE) na área relacionada ao procedimento, em atenção à solicitação do médico assistente.
Telecirurgia	Realização de procedimento cirúrgico a distância, com utilização de equipamento robótico e mediada por tecnologias interativas segura.
Telemonitoramento ou televigilância	Ato realizado sob coordenação, indicação, orientação e supervisão por médico para monitoramento ou vigilância a distância de parâmetros de saúde e/ou doença, por meio de avaliação clínica e/ou aquisição direta de imagens, sinais e dados de equipamentos e/ou dispositivos agregados ou implantáveis nos pacientes em domicílio, em clínica médica especializada em dependência química, em instituição de longa permanência de idosos, em regime de internação clínica ou domiciliar ou no translado de paciente até sua chegada ao estabelecimento de saúde.
Teletriagem	Ato realizado por um médico, com avaliação dos sintomas do paciente, a distância, para regulação ambulatorial ou hospitalar, com definição e direcionamento do paciente ao tipo adequado de assistência que necessita ou a um especialista.
Teletriagem	Ato realizado por um médico, com avaliação dos sintomas do paciente, a distância, para regulação ambulatorial ou hospitalar, com definição e direcionamento do paciente ao tipo adequado de assistência que necessita ou a um especialista.
Teleconsultoria	Ato de consultoria mediado por TDICs entre médicos, gestores e outros profissionais, com a finalidade de prestar esclarecimentos sobre procedimentos administrativos e ações de saúde.

Para todas as modalidades mencionadas acima, a Resolução CFM nº 2.134/2022 exige que seja assegurado ao paciente, ou seu representante legal, a obtenção do seu consentimento explícito. Assim, as pessoas devem estar conscientes "de que suas informações pessoais podem ser compartilhadas e sobre o seu direito de negar permissão para isso, salvo em situação de emergência médica" (Art. 15, parágrafo único, da Resolução CFM nº 2.134/2022).

Além disso, deve-se garantir ao paciente o Termo de Consentimento Livre e Esclarecido para a Teleconsulta (Art. 6º, § 5º, da Resolução CFM nº 2.134/2022). Neste documento é recomendável o fornecimento de explicações sobre o procedimento a ser realizado, com indicação de que são adotadas medidas de segurança para a proteção de dados, e os direitos do paciente e do médico, a exemplo de poderem optar, a qualquer momento, pela realização de atendimento presencial.

Ainda de acordo com a resolução, a telessaúde é compreendida como complementar ao tratamento

de qualquer paciente, sendo as consultas presenciais "o padrão ouro de referência" no atendimento ao paciente (Art. 6º, §1º, da Resolução CFM nº 2.134/2022).

Apesar das diferenças de modalidades da telessaúde, é possível identificar os principais tipos de dados pessoais no uso de serviços de telessaúde:

Dados de informação do paciente	Nome, data de nascimento, RG ou outro documento que comprove a identidade do paciente (e de seu responsável legal, caso aplicável), código do plano de saúde ou outra credencial, e-mail, telefone, imagem e voz.
Dados de saúde	Registro e avaliação de anamnese, exame objetivo e variáveis clínicas, prescrição de medicamentos ou outros métodos terapêuticos, informações sobre alergias e resultados de exames.
Dados de identificação do profissional de saúde responsável pelo atendimento do paciente	Nome, registro profissional, especialidade (se o caso), e-mail, telefone, imagem e voz.

No caso de teleatendimento que envolva menores de idade, os profissionais devem, no início do atendimento, informar ao responsável legal que este deverá acompanhar todo o processo de atendimento e ambas as pessoas devem seguir visíveis para o profissional até o fim do atendimento.

Por fim, cabe reforçar a competência do profissional responsável pelo atendimento e prestação do serviço quanto à avaliação se as modalidades de telessaúde são adequadas para atender às necessidades do paciente em cada situação específica.

6.3 RELAÇÃO COM TERCEIROS

O compartilhamento de dados pessoais no setor da saúde, entre os atores do setor e outros entes externos do setor privado e público, quando necessário, pode envolver, por exemplo, ações para desenvolver melhorias na qualidade do atendimento ao paciente, para uso de empresas serviços de hospedagens (como hardware, sistemas, softwares e infraestrutura necessária para manutenção dos dados e informações) e para atender a determinada obrigação legal.

Nestes casos, é possível citar a Resolução Normativa ANS nº 517/2022, que dispõe sobre as operações de compartilhamento da gestão de riscos envolvendo operadoras de planos de assistência à saúde, além da Resolução Normativa ANS nº 593/2023, que entrou em vigor em 1º de setembro de 2024, que busca promover a interoperabilidade e o compartilhamento de dados entre operadoras de planos de saúde e prestadores de serviços.

Outro exemplo se refere à Resolução Normativa nº 305/2012 da ANS, que define o protocolo TISS (Troca de Informações na Saúde Suplementar), com regras para o compartilhamento de informações dos agentes da saúde suplementar, incluindo os dados de atenção à saúde prestada ao beneficiário de plano privado de assistência à saúde, oriundos na rede de prestadores de serviços de saúde da operadora de planos privados de assistência à saúde. Nestes casos, o compartilhamento pode ser necessário para a aprovação de procedimentos de saúde. Em atenção ao princípio da necessidade e minimização, podem ser exigidos os dados cadastrais e de convênio, além das informações para execução do serviço conforme pedido médico, evitando a coleta de dados desnecessários, excessivos e sem justificativa legal.

A Resolução Normativa ANS nº 503/2022, ao dispor sobre as regras para celebração dos contratos escritos firmados entre as operadoras de planos de assistência à saúde e os prestadores de serviços de atenção à saúde, também apresenta orientações quanto ao compartilhamento de dados entre o setor privado de saúde. Um dos exemplos se refere à vedação para que sejam definidas regras que limitem o prestador de realizar auditorias técnicas ou administrativas de rotina, inclusive sobre o acesso às justificativas das glosas (Art. 5º, V). Além disso, os contratos devem expressamente prever que o compartilhamento de dados de atenção à saúde dos beneficiários de plano privado de assistência à saúde entre a operadora e o prestador só deve ocorrer de acordo com o Padrão TISS vigente (Art. 6º).

O respeito ao envio das informações no padrão TISS é de suma importância para a cadeia de saúde, uma vez que promove a padronização de dados e o formato que os dados serão compartilhados. Nesse sentido, qualquer solicitação ou envio de dados que extrapolem as previsões regulatórias vigentes deverão ser acordadas entre os atores, bem como observar os princípios e bases legais da LGPD.

Na relação entre distribuidores de produtos

de saúde e outros atores do setor de saúde, é possível haver o compartilhamento de dados do paciente e do profissional de saúde, como o nome e a informação do procedimento realizado, caso seja necessário um atendimento direcionado ou para solucionar eventuais reclamações quanto ao produto. Nestes casos, as medidas para minimização das informações utilizadas, bem como medidas de pseudonimização e cláusulas contratuais que garantam a segurança das informações são bons parâmetros para proteger a privacidade e os dados pessoais.

Além disso, para a operacionalização dos serviços contratados por pacientes, as cláusulas contratuais entre os agentes do setor de saúde podem conferir maior segurança jurídica no compartilhamento de dados pessoais. No caso das atividades de corretoras, os dados de identificação do paciente (como nome, e-mail, telefone, idade e CEP) podem ser utilizados para intermediar o contato com as operadoras de saúde, e devem atender às condições de legitimidade para permitir o tratamento lícito e legal dos dados conforme a LGPD.

A seguir, há outras possibilidades de compartilhamento de dados entre o setor privado de saúde:

EXEMPLOS DE COMPARTILHAMENTO DE DADOS ENTRE O SETOR PRIVADO DA SAÚDE

- Antes da realização de procedimentos, prestadores de serviços de saúde podem compartilhar com operadoras de planos de saúde, fornecedores e distribuidores os dados pessoais e clínicos do paciente para a autorização do procedimento, cotação e agendamento.
- No credenciamento e prestação de serviços, dados podem ser compartilhados entre prestadores de serviços de saúde e operadoras de planos de saúde para oferecer opções aos consumidores.
- Operadoras de planos de saúde e prestadores de serviços de saúde podem compartilhar informações sobre pedidos de exames e procedimentos para o faturamento de guias.
- Dados pessoais, inclusive sensíveis do paciente e dados de identificação do profissional de saúde podem ser compartilhados entre operadoras de planos de saúde e fornecedores de produtos de saúde para cotação, agendamento, remessa e faturamento de produtos utilizados em cirurgias.
- Para viabilizar a entrega de medicamentos e equipamentos, prestadores de serviços de saúde podem compartilhar dados de pacientes (como prescrição médica) com fornecedores ou distribuidores desses produtos.
- Operadoras de planos de saúde podem realizar auditorias para verificar a conformidade dos procedimentos realizados pelos prestadores de serviços de saúde.
- Prestadores de serviços de saúde podem compartilhar dados pessoais dos pacientes com as Operadoras de planos de saúde para fins de faturamento do serviço e apuração de uso dos serviços de forma agregada.

O compartilhamento de dados pessoais deve respeitar as condições de legitimidade do tratamento, sendo limitado ao mínimo necessário para alcançar a finalidade específica, evitando a coleta de dados excessivos ou inadequados. Além disso, considerando a sensibilidade dos dados tratados, sua frequência e compartilhamento com diversos stakeholders, os titulares devem ser informados de forma clara sobre a operação.

BOAS PRÁTICAS PARA O COMPARTILHAMENTO DE DADOS PESSOAIS

- Avalie cuidadosamente se o compartilhamento é necessário e se atende às condições de legitimidade definidas pela LGPD (conformidade com os princípios e bases legais).
- Certifique-se se o compartilhamento é realizado de forma legítima e lícita, com fundamento em uma das bases legais dispostas nos arts. 7º e 11 da LGPD;
- Explique de forma clara e acessível aos titulares a existência ou não de compartilhamento, com o fornecimento de informações relevantes que justificam o tratamento de dados.
- Mantenha o registro das informações, incluindo a documentação dos processos e com quem há o compartilhamento, seja quando sua empresa envia ou recebe dados de terceiros.
- Implemente cláusulas em contratos com terceiros sobre compartilhamento de dados pessoais.
- Priorize o uso de medidas de pseudonimização, anonimização e adote ações para criptografia das informações.
- Utilize sistemas dispositivos seguros e mantenha o controle de acesso e de ações, para evitar incidentes de segurança.

Abaixo, algumas informações essenciais para a contratualização de compartilhamento de dados na saúde:

RECOMENDAÇÕES CONTRATUAIS COM PARCEIROS SOBRE PROTEÇÃO DE DADOS PESSOAIS

- Indique o glossário com terminologia da LGPD.
- Acorde sobre a duração das atividades de tratamento.
- Identifique os agentes de tratamento, com respectivas atribuições e responsabilidades.
- Defina as finalidades específicas do tratamento de dados.
- Preveja a possibilidade de proibição da utilização de dados pessoais sem ciência ou autorização da instituição controladora.
- Exija a adequação das partes do contrato à LGPD.
- Vede o compartilhamento de dados pessoais e obrigatoriedade de notificação à parte caso o compartilhamento seja necessário.
- Defina a obrigação de registro de informações e de implementação de medidas técnicas e administrativas que garantam a segurança dos dados e das informações compartilhadas.
- Preveja a possibilidade de realização de auditorias para demonstração de cumprimento da legislação.
- Indique os deveres de confidencialidade que devem ser observados.
- Estipule a periodicidade de atualização de informações do contrato.
- Defina prazos para a notificação de eventuais incidentes e a abstenção de comunicação às autoridades ou aos titulares sem a prévia autorização da outra parte.
- Defina prazos para a notificação em caso de exercício de direitos dos titulares e cooperação na resposta aos titulares e autoridades se for o caso.
- Adote as cláusulas padrão de transferência internacional de dados se for um contrato que envolve este tipo de operação.
- Verifique as possibilidades de cooperação entre as partes para atendimento aos direitos dos titulares e determinações de autoridades, com definições sobre obrigatoriedade de notificação em caso de determinações oficiais que obriguem o fornecimento de dados pessoais.
- Indique a obrigatoriedade de contratação de encarregado por operador ou, se aplicável, o canal de comunicação com o titular.
- Em caso de compartilhamento de dados, inclua a previsão de procedimentos para devolução de dados pessoais e exclusão definitiva.
- Preveja a realização de diligência prévia e contínua do terceiro contratado, para que sejam atestadas o cumprimento à LGPD.

Outro ponto que merece atenção se refere à possibilidade de compartilhamento de dados fora do território brasileiro, a chamada transferência internacional de dados. A transferência internacional ocorre quando o exportador (agente de tratamento, localizado no Brasil ou em outro país, que transfere dados pessoais) transferir dados pessoais para o importador (agente de tratamento, localizado em país estrangeiro ou que seja organismo internacional, que recebe dados pessoais transferidos por exportador), conforme as definições da Resolução CD/ANPD nº 19/2024, que estabelece o Regulamento de Transferência Internacional de Dados.

De acordo com a Resolução CD/ANPD nº 19/2024, em todas as hipóteses que autorizam a transferência internacional, é importante que a atividade se limite “ao mínimo necessário para o alcance de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados” (Art. 9º, § único, da Resolução CD/ANPD nº 19/2024). Ademais, cabe ao controlador, avaliar a hipótese que sustenta a atividade de tratamento nos termos do Art 33 da LGPD, selecionando o mecanismo de transferência internacional válido a legitimar essa operação (Ar. 4º, I a III, da Resolução CD/ANPD nº 19/2024).

Para assegurar que se tenha o compartilhamento de dados pessoais entre terceiros é necessário que todo o processo seja realizado de forma transparente, segura e ética, em conformidade com a legislação vigente. A LGPD e as determinações da ANPD, nesse contexto, desempenham um papel crucial ao estabelecer um marco regulatório que equilibra os interesses dos pacientes, das empresas e da sociedade como um todo, garantindo a proteção dos dados pessoais e a promoção da inovação no setor da saúde.

6.4 PREVENÇÃO E PROMOÇÃO DE SAÚDE

As atividades de prevenção e promoção de saúde são as ações estratégicas que têm como objetivo manter e melhorar a saúde da população, além de prevenir doenças e promover estilos de vida saudáveis. Essas atividades podem ser individuais, comunitárias ou de âmbito governamental, englobando uma ampla gama de ações, desde a educação em saúde até o apoio na criação de políticas públicas.

Para estes objetivos, o tratamento de dados pode ocorrer no âmbito da prestação de serviços de saúde, na saúde suplementar e para a produção e disponibilização de dispositivos médicos. Dentre as possíveis finalidades de tratamento para prevenção e promoção da saúde, é possível indicar:

POSSIBILIDADES DE TRATAMENTO DE DADOS **PESSOAIS PARA PREVENÇÃO E PROMOÇÃO DE SAÚDE**

- **Identificação de grupos de risco:** através da análise de dados demográficos, históricos de saúde e fatores de risco, é possível identificar grupos populacionais mais vulneráveis a determinadas doenças ou condições de saúde. Isso permite direcionar ações preventivas e de promoção da saúde de forma mais eficaz.
- **Monitoramento de doenças crônicas:** dados sobre doenças crônicas, como diabetes e hipertensão, permitem acompanhar a evolução da doença, identificar complicações e ajustar os tratamentos de forma personalizada.
- **Avaliação da eficácia de intervenções:** ao coletar dados sobre os resultados de programas e intervenções de saúde, é possível avaliar sua eficácia e realizar ajustes para otimizar os resultados.
- **Personalização de cuidados:** é possível oferecer cuidados de saúde mais personalizados, considerando as necessidades e características de cada paciente.
- **Educação em saúde:** dados sobre hábitos e estilos de vida podem ser usados para desenvolver programas educacionais personalizados que ajudam as pessoas a adotarem comportamentos mais saudáveis.
- **Planejamento de recursos de saúde:** os dados agregados de uma população podem ser analisados para planejar a alocação de recursos, como em hospitais, clínicas, e para a indicação de profissionais de saúde em áreas onde são mais necessários. Além disso, é possível que se tenha previsão de demandas, permitindo que os sistemas de saúde se preparem melhor para eventuais picos de demanda.
- **Avaliação de desempenho do sistema de saúde:** os resultados de saúde podem ser utilizados para avaliação da eficácia dos serviços de saúde e fazer ajustes necessários para melhorar a qualidade do atendimento.
- **Pesquisas científicas:** os dados agregados e anonimizados são utilizados em pesquisas científicas para o desenvolvimento de novos tratamentos, medicamentos e tecnologias.
- **Desenvolvimento de políticas públicas:** os dados sobre a saúde da população são utilizados para embasar a formulação de políticas públicas de saúde, direcionando os recursos para as áreas mais necessitadas.

Para tanto, as avaliações das condições de legitimidade do tratamento são relevantes não apenas para garantir a proteção de dados, como resguardar a autonomia dos titulares e garantir o compartilhamento seguro entre os entes envolvidos na atividade.

Essa autonomia e envolvimento do titular é essencial para que o indivíduo possa exercer seus direitos, como acesso, correção e eliminação de dados, além de permitir uma relação transparente e equilibrada. Em um cenário de crescente digitalização e processamento massivo de informações, assegurar que o titular mantenha o controle sobre seus próprios dados fortalece a proteção da privacidade e a confiança no tratamento responsável por parte das organizações. Assim, deve-se evitar a coleta extensiva de dados pessoais e assegurar que todo o tratamento se limite apenas ao específico e necessário para a finalidade legal e lícita definida.

Os princípios da adequação e necessidade merecem atenção porque cabe aos agentes de tratamento garantirem que os dados pessoais tratados serão proporcionais, adequados para a finalidade proposta e que o titular tenha a expectativa de que os seus dados serão utilizados para a finalidade que lhe foi informada. Estes princípios também devem orientar as definições do tempo de armazenamento e exclusão dos dados por parte dos agentes de tratamento.

Além disso, as instituições devem implementar medidas de segurança técnica aptas a prevenir eventuais incidentes de dados, como a criptografia e restrição de acesso às informações. Nesse sentido, reforça-se a importância da anonimização e pseudonimização dos dados, que devem ser adotadas sempre que possível.

O princípio da não discriminação também precisa ser seguido em todas as etapas do tratamento de dados, para que não sejam realizadas operações

que possam prejudicar ou segregar, de forma ilícita ou abusiva, indivíduos. No caso de tratamento que envolva dados pessoais sensíveis, deve-se adotar maior cautela já que, por si só, possuem maior tendência de poderem gerar alguma discriminação.

Ademais, quando a atividade puder gerar risco relevante para os titulares de dados, é recomendável a elaboração do Relatório de Impacto à Proteção de Dados (RIPD), já que é um documento que busca prever e evitar os riscos, e não somente mitigá-los após a sua ocorrência.

BOAS PRÁTICAS DE TRATAMENTO DE DADOS **PESSOAIS PARA PREVENÇÃO E PROMOÇÃO DE SAÚDE**

- Sempre que possível, opte pelo uso de dados anonimizados e pseudonimizados.
- Mantenha os dados coletados pelo menor tempo possível e os elimine quando não forem necessários.
- Ao analisar as condições de legitimidade para o tratamento de dados, certifique-se de documentar os meios utilizados para análise do fluxo de dados e avaliação de risco. Exemplos neste sentido são o Teste de Balanceamento do Legítimo Interesse e a elaboração do Relatório de Impacto à Proteção de Dados Pessoais.
- Adote a privacidade por design desde o início do desenvolvimento de sistemas e processos.
- Estabeleça ações de controle e gerenciamento de acesso aos dados pessoais e informações utilizadas, limitando aos profissionais competentes através do monitoramento de acesso, técnicas de permissões granularizadas e autenticação multifator.
- Implemente medidas técnicas e administrativas robustas para proteção dos dados contra acessos não autorizados, perdas e demais formas de incidentes.
- Em casos de compartilhamento, realize diligências prévias com os terceiros e estabeleça contratos com cláusulas específicas para garantia da proteção de dados e confidencialidade das informações.
- Realize periodicamente ações de revisão e avaliação de risco, para prevenção, melhoria e adequação das práticas adotadas pela instituição.

Por fim, para efetivar o princípio da transparência os titulares devem ser informados claramente sobre como os seus dados podem ser utilizados, com a identificação de quais categorias e tipo de dados são necessários e quais as respectivas finalidades, além de quais outros entes podem acessá-los neste processo. Eventuais atualizações devem ser amplamente divulgadas e destacadas aos titulares, o que pode ocorrer através da divulgação nos principais meios de comunicação com os titulares e disponibilização das informações no sítio eletrônico da instituição.

Assim, observa-se que a proteção de dados é um elemento fundamental para a prevenção e promoção da saúde. Ao garantir a privacidade e a segurança dos dados pessoais, é possível o tratamento de dados seguro para benefício da saúde dos titulares, com respeito à transparência, ética e inovação.

6.5 REALIZAÇÃO DE AUDITORIAS

As auditorias são ferramentas essenciais de gestão e fiscalização, internas ou independentes, que analisam as condutas e procedimentos adotados pela instituição. O principal objetivo é identificar irregularidades ou inconsistências em relação às leis e regras aplicáveis, permitindo intervenções para correção, readequação e melhorias nos custos e na qualidade da assistência à saúde. Elas podem envolver diversas áreas da instituição, como recursos humanos e finanças.

No setor de saúde, as auditorias podem avaliar a prestação de serviços, contas e procedimentos em hospitais, operadoras de planos de saúde, consultórios e clínicas, visando prevenir e combater o uso indevido dos serviços. Para as operadoras de planos de saúde, em especial, as auditorias verificam se os serviços autorizados foram realmente prestados. Além disso, podem abranger atividades operacionais, como a correção de duplicações indevidas de contas e o cumprimento de protocolos e condutas estabelecidas.

Auditoria de contas médicas

A Resolução Normativa DC/ANS nº 503 de 30/03/2022, ao dispor sobre as regras para celebração dos contratos escritos firmados entre as operadoras de planos de assistência à saúde e os prestadores de serviços de atenção à saúde, orienta que os contratos devem prever expressamente a rotina de auditoria administrativa e técnica. O Art. 14 da mencionada Resolução, inclui, por exemplo, a previsão quanto aos prazos para contestação da glosa, para resposta da operadora e para pagamento dos serviços em caso de revogação da glosa aplicada (Art. 14, II); e a conformidade com a legislação específica dos conselhos profissionais sobre o exercício da função de auditor (Art. 14, III).

Assim, podem ser tratados documentos como:

EXEMPLOS DE INFORMAÇÕES NECESSÁRIAS PARA **A REALIZAÇÃO DE AUDITORIAS**

- Registros e documentos técnicos-administrativos.
- Prontuários para análise de cumprimento de protocolos.
- Avaliação de documentos, como receitas médicas, para análise da compatibilidade de gastos com exames e medicamentos com a quantidade de atendimentos.
- Análise prévia das contas a serem enviadas aos pacientes ou operadoras, para avaliação dos serviços prestados e eventual correção no faturamento.

Há ainda a previsão do cargo de médico auditor, conforme orientações da Resolução CFM nº 1.614/2001. A Resolução apresenta as seguintes orientações quando à conduta dos profissionais em serviços de auditoria médica:

REQUISITOS PARA REALIZAÇÃO DE AUDITORIAS MÉDICAS

- O médico, na função de auditor, deve identificar-se, de forma clara, em todos os seus atos, fazendo sempre constar o número de seu registro no Conselho Regional de Medicina (Art. 3º, da Resolução CFM nº 1.614/2001).
- O médico, na função de auditor, deve se apresentar ao diretor técnico ou substituto da unidade, antes do início de suas atividades (Art. 4º, da Resolução CFM nº 1.614/2001).
- O médico, na função de auditor, se obriga a manter o sigilo profissional e deve, sempre que necessário, comunicar a quem de direito e por escrito suas observações, conclusões e recomendações, sendo-lhe vedado realizar anotações no prontuário do paciente (Art. 6º, da Resolução CFM nº 1.614/2001).
- O diretor técnico ou diretor clínico deve garantir ao médico/equipe auditora todas as condições para o bom desempenho de suas atividades, bem como o acesso aos documentos que se fizerem necessários (Art. 5º, da Resolução CFM nº 1.614/2001).
- O médico, na função de auditor, tem o direito de acessar, in loco, toda a documentação necessária, sendo-lhe vedada a retirada dos prontuários ou cópias da instituição, podendo, se necessário, examinar o paciente, desde que devidamente autorizado pelo mesmo, quando possível, ou por seu representante legal (Art. 7º, da Resolução CFM nº 1.614/2001).
- O médico, na função de auditor, quando integrante de equipe multiprofissional de auditoria, deve respeitar a liberdade e independência dos outros profissionais sem, todavia, permitir a quebra do sigilo médico (Art. 10, da Resolução CFM nº 1.614/2001).

Auditorias Internas

No caso de auditores internos, o Instituto dos Auditores Internos do Brasil (IIA Brasil) apresenta em seu Código de Ética as seguintes regras de conduta, que podem ser aplicáveis aos processos de auditoria independente da área de especialização:

REGRAS APLICÁVEIS AO AUDITOR INTERNO, DE ACORDO COM A IIA BRASIL

Princípio da integridade

- executar seus trabalhos com honestidade, diligência e responsabilidade.
- observar a lei e fazer as divulgações esperadas pela legislação e pela profissão.
- não deve conscientemente fazer parte de qualquer atividade ilegal ou se envolver em atos impróprios para a profissão de Auditoria Interna ou para a organização.
- respeitar e contribuir para os objetivos legítimos e éticos da organização.

Princípio da objetividade

- não deve participar de qualquer atividade ou relacionamento que possa prejudicar ou que presumidamente prejudicaria sua avaliação imparcial. Esta participação inclui aquelas atividades ou relacionamentos que possam estar em conflito com os interesses da organização.
- não devem aceitar qualquer coisa que possa prejudicar ou que presumidamente prejudicaria seu julgamento profissional.
- divulgar todos os fatos materiais de seu conhecimento que, caso não sejam divulgados, possam distorcer o reporte sobre as atividades sob revisão

Princípio da confidencialidade

- ser prudente no uso e proteção das informações obtidas no curso de suas funções.
- não deve utilizar informações para qualquer vantagem pessoal ou de qualquer outra maneira contrária à lei ou em detrimento dos objetivos legítimos e éticos da organização.

Princípio da competência

- se envolver somente com aqueles serviços para os quais possuam os necessários conhecimentos, habilidades e experiência.
- executar os serviços de Auditoria Interna em conformidade com as Normas Internacionais para a Prática Profissional de Auditoria Interna.
- melhorar continuamente sua proficiência, e a eficácia e qualidade de seus serviços.

Disponível em: https://iiabrasil.org.br/ippf/codigo-de-etica.

Diante da possibilidade de os documentos analisados em auditorias conterem dados pessoais, é essencial que as instituições se adequem à LGPD. Embora a ANPD ainda não tenha emitido orientações específicas para auditorias, as instituições devem definir uma periodicidade, como auditorias anuais, para prevenir incidentes de segurança e garantir a integridade dos dados. Além disso, tais procedimentos podem estar previstos em contratos para conferir maior segurança para todas as partes envolvidas.

A padronização na coleta e armazenamento de dados também aumenta a segurança, assegurando que a coleta seja feita de forma específica e limitada às finalidades da auditoria. Para proteger a privacidade dos titulares, é importante adotar medidas como pseudonimização e anonimização dos dados, além de restringir o acesso às informações apenas aos auditores autorizados. Documentar os processos de auditoria e definir prazos para armazenamento e exclusão de dados pessoais são práticas fundamentais para comprovar a conformidade com a LGPD.

Outras medidas incluem a elaboração de políticas e procedimentos internos com boas práticas, além de investir em treinamentos periódicos para capacitar as equipes e reduzir riscos, garantindo a conformidade com as normas e regulamentações do setor.

O estabelecimento da regularidade de auditorias em programas de governança de privacidade contribui para o monitoramento contínuo das instituições, conforme previsto no Art. 50, §2º, I, d e h, da LGPD, que recomenda políticas e salvaguardas baseadas em avaliações sistemáticas de impactos e riscos à privacidade.

Após a auditoria, os responsáveis devem avaliar a necessidade de medidas como a elaboração de relatórios que detalhem as medidas de segurança aplicadas e os resultados obtidos, além da exclusão segura de dados desnecessários, utilizando métodos que garantam a eliminação completa das informações.

6.6 UTILIZAÇÃO DE FERRAMENTAS DE IDENTIFICAÇÃO

O uso de ferramentas de identificação no setor de saúde é variado, mas podemos destacar duas importantes finalidades: (i) promover o controle de acesso e a segurança, e (ii) auxiliar no combate a fraudes, especialmente em planos de saúde.

Dentre as ferramentas utilizadas para assegurar a identificação das pessoas no controle de acesso e para prevenir fraudes contratuais:

FERRAMENTAS PARA **IDENTIFICAÇÃO USADAS NO SETOR DE SAÚDE**

Controle de acesso	Cartões de acesso: cartões personalizados, como crachás, podem envolver o uso do nome, cargo profissional ou indicação do vínculo com paciente (se acompanhante ou responsável legal), código de verificação próprio da instituição, foto, horário e data de registro na recepção. Códigos de barras ou RFID (Radio Frequency Identification - identificação por radiofrequência): podem ser usados em chips, pulseiras ou etiquetas para confirmação da identidade de pacientes. Biometria: que pode envolver a análise da impressão digital, reconhecimento facial ou de voz, por exemplo, para controle de acesso a áreas restritas e controle de ponto de funcionários.
Prevenção à fraude contratual	Onboarding digital: a biometria facial e a digital podem ser usadas para verificar a identidade de novos clientes durante o processo de cadastro, reduzindo o risco de fraudes por identidade. Uso combinado de biometria e assinatura eletrônica: a biometria facial e a

assinatura digital podem ser combinadas para criar um processo de assinatura eletrônica mais seguro, evitando fraudes em contratos digitais.

Leitura de OCR (Optical Character Recognition): a análise de imagens e identificação de padrões em um documento podem ser usadas para coibir a entrada e faturamento de pedidos de reembolso fraudulentos.

Para permitir o controle de acesso e garantir a segurança, as ferramentas de identificação desempenham um papel crucial tanto em ambientes físicos quanto em plataformas digitais, como aplicativos. No acesso a locais físicos, essas ferramentas permitem restringir o acesso a áreas sensíveis, minimizando o risco de acesso não autorizado a informações confidenciais.

Nos serviços digitais, como aplicativos de saúde ou plataformas de prontuário eletrônico, o uso de autenticação multifatorial e senhas fortes é igualmente importante para garantir que apenas indivíduos autorizados, como funcionários, pacientes e terceiros devidamente credenciados, possam acessar os dados. Essas medidas de controle não apenas protegem a integridade das informações pessoais, mas também ajudam a prevenir incidentes de segurança, como vazamento ou uso indevido de dados pessoais sensíveis.

Já em relação ao combate às fraudes em planos de saúde, a importância das ferramentas de identificação é evidente diante do contexto enfrentado pelo setor de saúde no Brasil.

Entre as principais fraudes cometidas contra operadoras de planos de saúde estão: (i) fraude em reembolso, onde os dados dos titulares são usados por golpistas para solicitar reembolsos indevidos e lucrar com o aumento do preço do serviço; (ii) fraude em boleto, onde as informações no boleto de pagamento são alteradas e o valor é pago aos golpistas; (iii) tentativas de burlar os sistemas de identificação, seja por falsificação de documentos ou fraude biométrica.

Nesse sentido, as ações proteção aos titulares e prevenção à fraude tem mobilizado o setor de saúde a desenvolver iniciativas de conscientização, como o exemplo da campanha “Saúde Sem Fraude”.

Considerando a importância das medidas de identificação para prevenir acessos indevidos e combater fraudes, os responsáveis pelo tratamento de dados pessoais devem avaliar a utilização dessas medidas e a garantia de que o tratamento de dados seja limitado ao mínimo necessário para a finalidade pretendida. Sempre que possível, deve-se optar por técnicas menos invasivas à privacidade e aos direitos dos titulares.

Em todas as fases de tratamento, é fundamental observar os princípios da finalidade, necessidade, adequação, transparência e não-discriminação, incluindo a escolha da base legal adequada para o tratamento.

Nesse caso, a hipótese legal da prevenção à fraude e segurança do titular (Art. 11, II, g) pode ser aplicada, mas com parcimônia, já que ela é direcionada a promover o benefício do próprio titular. As finalidades das atividades definidas pelo controlador devem ser restritas à prevenção de fraudes e à promoção da segurança do titular, sem desvios de propósito.

Dessa forma, como boas práticas, podem ser recomendadas as seguintes orientações:

BOAS PRÁTICAS PARA O USO **DE FERRAMENTAS DE IDENTIFICAÇÃO**

- Identifique previamente a categoria de dados pessoais envolvidos e os titulares alcançados, para que a coleta de dados seja realizada apenas se estritamente necessário.
- Quando possível, utilize técnicas menos invasivas para identificação dos titulares.
- Adote as medidas de pseudonimização e criptografia de dados, para garantir a segurança das informações e dados dos titulares.
- Realize avaliações de risco para as atividades, com a elaboração do Relatório de Impacto à Proteção de Dados (RIPD), quando necessário.
- Providencie materiais informativos de forma clara, acessíveis e transparentes quanto às tecnologias utilizadas e quais os objetivos que justificam o seu uso.
- Defina políticas para retenção e descarte de dados, com definição de prazos para que ocorra o armazenamento e exclusão seguros de dados pessoais desnecessários.
- Periodicamente realize atividades de monitoramento e revisão para identificar e corrigir vulnerabilidades, revisão de documentos, como o RIPD, bem como por meio de auditorias regulares.
- Portanto, é necessário que, neste processo de avaliação e ponderação com os direitos dos titulares, as instituições tenham clareza dos motivos que justificaram a escolha dos métodos utilizados, para assegurar a proteção de dados pessoais e comprovarem a conformidade com a LGPD, inclusive para fins de auditoria.

7. PEQUENOS E MÉDIOS AGENTES DE TRATAMENTO

O processo de adequação à LGPD deve ser adaptado à realidade de cada instituição e não precisa ser oneroso. Em razão de abranger um grupo mais reduzido de pessoas, é possível ainda que as pequenas e médias empresas implementem mais facilmente medidas em prol da cultura de proteção de dados pessoais. Como ações prioritárias que devem ser adotadas pelas organizações, é possível indicar:

SEIS FASES PRIORITÁRIAS PARA **ADEQUAÇÃO À LGPD**

1) Mapeamento das atividades de tratamento de dados pessoais	· Identifique todos os tratamentos de dados pessoais realizados pela sua instituição. · Defina para cada tratamento uma base legal para o tratamento, incluindo para compartilhamento com outras empresas. Colete o consentimento do titular de dados quando este for o caso. · Defina o prazo e armazenamento e retenção de cada tipo de dado pessoal conforme as orientações legais. · Mantenha o Registro das Operações de Tratamento de Dados (RoPA) atualizado.
2) Análise de riscos (gap analysis)	· Avalie quais são as práticas adotadas pela empresa que já estão em conformidade com a Lei e quais precisam ser aprimoradas. Nesta etapa, a empresa deverá identificar quais são as áreas com mais prioridade de adequação e que tendem a representar maior vulnerabilidades. · Descarte informações antigas que não são mais necessárias.
3) Estruturação da governança em privacidade	· Defina o plano de adequação para atingir os objetivos da adequação à LGPD. · Estabeleça controles de acesso para que apenas pessoas autorizadas possam acessar os dados pessoais.
4) Revisão contratual e de outros documentos	· Nesta fase é possível a indicação do encarregado de dados ou do canal de comunicação com o titular, como previsto pela Resolução CD/ANPD nº 2/2022 · Elabore cláusulas contratuais sobre proteção de dados pessoais, que devem ser utilizadas para a atualização de documentos já existentes e ser incluídas a partir desse momento.
5) Atendimento aos direitos dos titulares de dados	· Garanta o exercício de direitos previstos na LGPD pelos titulares de dados, que pode ser organizado com apoio da gestão do canal de comunicação com os titulares de dados da gestão do canal de comunicação com os titulares de dados.
6) Treinamento	· Capacite seus funcionários conforme as orientações da LGPD e considere as suas atividades diárias para instruí-los de forma específica. Os funcionários da sua empresa são essenciais para o sucesso da adequação à LGPD e para a implementação da nova cultura de proteção de dados em toda a organização.

CIPL. CEDIS IDP. Prioridades das Organizações Públicas e Privadas Implementarem de Forma Eficaz a Nova Lei Geral Brasileira de Proteção de Dados (LGPD). 2020. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/%5bpt%5d_cipl-idp_white_paper_on_top_priorities_for_organizations_to__effectively_implement_the_lgpd_7_october_2020_.pdf.

No caso das pequenas e médias empresas (PMEs), em 2022, a ANPD publicou a Resolução CD/ANPD nº 2/2022 a qual, em seu artigo 2º, II, inclui para a categoria de agentes de tratamento de pequeno porte os seguintes grupos que assumam obrigações típicas de agentes de tratamento: microempresas, empresas de pequeno porte, startups, pessoas jurídicas de direito privado, inclusive sem fins lucrativos.

QUEM SÃOS OS AGENTES DE PEQUENO PORTE CONFORME A RESOLUÇÃO CD/ANPD Nº 2/2022?

Empresas de pequeno porte

Lei Complementar nº 123/2006

- Ser sociedade empresária, sociedade simples, sociedade limitada unipessoal devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas.
- Auferir, em cada ano-calendário, receita bruta superior a R$ 360.000,00 e igual ou inferior a R$ 4.800.000,00.

Microempreendedor individual

Lei Complementar nº 123/2006

- Ser sociedade empresária, sociedade simples, sociedade limitada unipessoal devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas.
- Auferir, no ano-calendário anterior, de até R$ 81.000,00.
- Não ter filiais.
- Não ser sócio ou administrador de outra empresa.
- Atuar nas ocupações permitidas pelo Anexo XI da Resolução CGSN nº 140, de 2018.

Microempresas

Lei Complementar nº 123/2006

- Ser sociedade empresária, sociedade simples, sociedade limitada unipessoal devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas.
- Auferir, em cada ano-calendário, receita bruta igual ou inferior a R$ 360.000,00.

Startups

Lei Complementar nº 182/2021

- Empresário individual, empresa individual de responsabilidade limitada, sociedades empresárias, sociedades cooperativas e sociedades simples.
- Receita bruta de até R$ 16.000.000,00 no ano-calendário anterior ou de R$ 1.333.334,00 multiplicado pelo número de meses de atividade no ano-calendário anterior, quando inferior a 12 meses.
- Recém-inauguradas em operação recente (até 10 anos de inscrição no CNPJ.
- Atuação caracterizada pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados ou enquadramento no regime especial Inova Simples.

A Resolução CD/ANPD nº 2/2022 detalha que, se observados os seguintes requisitos, não poderão se beneficiar do tratamento diferenciado quem:

- Realizar tratamento de alto risco para os titulares, exceto quando agentes de pequeno porte estiverem organizados por entidades de representação para mediação de reclamações (Art. 8º, Resolução CD/ANPD nº 2/2022).
- Para startups, auferir receita bruta superior a R$ 16 milhões no ano anterior ou a R$ 1.333.334,00 multiplicado pelos meses de atividade, se inferior a 12 meses (Lei Complementar nº 182, de 2021).
- Ter receita bruta anual entre R$ 360 mil e R$ 4,8 milhões para empresas de pequeno porte (Lei Complementar nº 123, de 2006, alterada pela Lei Complementar nº 155, de 2016).
- Pertencer a grupo econômico cuja receita global ultrapasse os limites dos itens anteriores.

Em razão dessas exceções, vale pontuar que, mesmo que sejam consideradas agentes de pequeno porte, muitas empresas do setor de saúde não podem se valer das flexibilizações detalhadas abaixo, como os hospitais de pequeno porte, porque tratam dados sensíveis (incluindo dados sensíveis de saúde) que podem, se violados, afetar significativamente os interesses e direitos fundamentais dos titulares, o que caracteriza tratamento de alto risco nos termos da Resolução CD/ANPD nº 2/2022

Para os agentes de tratamento de pequeno porte, a Resolução CD/ANPD nº 2/2022 dispõe da flexibilização das seguintes obrigações:

- a) Reclamações coletivas de titulares (Art. 8º): Agentes de pequeno porte, inclusive os que realizam tratamentos de alto risco, podem se organizar por meio de entidades representativas para negociar, mediar e conciliar reclamações de titulares de dados.
- b) Registro simplificado de operações de tratamento (Art. 9º): Podem cumprir a obrigação de manter o registro das operações de tratamento de dados de forma simplificada. A ANPD fornecerá um modelo para esse registro.
- c) Política simplificada de comunicação de incidentes de segurança (Art. 10): A comunicação de incidentes pode ocorrer de forma simplificada, conforme regulamentação específica.
- d) Dispensa de indicação do encarregado (Art. 11): Agentes de pequeno porte não são obrigados a indicar um encarregado de proteção de dados, mas devem estabelecer um canal de comunicação com os titulares. Caso optem pela indicação do encarregado, isso será considerado uma política de boas práticas.
- e) Política simplificada de segurança da informação (Art. 13): Deve atender aos requisitos essenciais para proteger dados pessoais contra incidentes de segurança.

Além disso, a Resolução CD/ANPD nº 2/2022 estabelece condições favoráveis a estes agentes em relação aos seguintes prazos:

SERÁ CONCEDIDO PRAZO EM DOBRO PARA:

Atendimento das solicitações dos titulares.

Comunicação da ocorrência de incidente de segurança à ANPD e ao titular, exceto quando houver potencial comprometimento à integridade física ou moral dos titulares ou à segurança nacional.

No fornecimento de declaração clara e completa que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, quando requisitados pelo titular.

Atenção:

Outros prazos para a apresentação de informações, documentos, relatórios e registros solicitados pela ANPD a outros agentes de tratamento.

Prazos estabelecidos nos normativos próprios para apresentação de informações, documentos, e relatórios solicitados pela ANPD a outros agentes de tratamento.

Os agentes de tratamento de pequeno porte podem fornecer a declaração simplificada do Art. 19, I, da LGPD no prazo de até 15 dias, contados da data do requerimento.

Em 2021, a ANPD publicou o Guia de Segurança da Informação para Agentes de Tratamento de Pequeno Porte e ressaltou que mesmo para estas organizações o gerenciamento de riscos na organização é uma etapa relevante para "identificar, quantificar e gerenciar os riscos relacionados à segurança da informação dentro da organização".

A Autoridade também recomenda que este gerenciamento ocorra periodicamente, pois é "parte integrante das práticas de gerenciamento", sendo "um importante elemento da boa governança" e colabora na organização interna e tomada de decisões.

A ANPD também disponibilizou em 2021 o Guia Orientativo "Segurança da informação para agentes de tratamento de pequeno porte", com um checklist de medidas de segurança para agentes de tratamento de pequeno porte:

CHECKLIST DE MEDIDAS DE SEGURANÇA PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE PREVISTOS PELA ANPD

Política de segurança da informação

- Estabelecer uma política de segurança da informação simplificada, que estabeleça controles relacionados ao tratamento de dados pessoais, como cópias de segurança, uso de senhas, acesso à informação, compartilhamento de dados, atualização de softwares, uso de correio eletrônico e uso de antivírus.
- Realizar revisões periódicas da política de segurança da informação.
- Gerenciar contratos e aquisições com observância ao tratamento adequado dos dados pessoais.

Conscientização e treinamento	Realizar a conscientização dos funcionários, via treinamentos e campanhas sobre as suas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais conforme disposto na LGPD e normas da ANPD. Informar e sensibilizar todos os funcionários da organização, especialmente aqueles diretamente envolvidos na atividade de tratamento de dados, sobre as obrigações legais existentes na LGPD e em normas e orientações editadas pela ANPD. • Informar os funcionários sobre: • como utilizar controles de segurança dos sistemas de TI relacionados ao trabalho diário; • como evitar de se tornarem vítimas de incidentes de segurança corriqueiros, tais como contaminação por vírus ou ataques de phishing, que podem ocorrer, por exemplo, ao clicar em links recebidos na forma de pop-up de ofertas promocionais ou em links desconhecidos que chegam por e-mail; • manter documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre as mesas; • não compartilhar logins e senhas de acesso das estações de trabalho; • bloquear os computadores quando se afastar das estações de trabalho, para evitar o acesso indevido de terceiros; • seguir as orientações da política de segurança da informação. Criar um ambiente organizacional que incentive usuários de sistemas da empresa, tanto clientes quanto funcionários, a informar incidentes e vulnerabilidades detectadas.
Gerenciamento de contratos	Estabelecer contratos com cláusulas de segurança da informação que assegurem a proteção de dados pessoais, tais como: • regras para fornecedores e parceiros; • regras sobre compartilhamentos; • relações entre controlador-operador; • orientações sobre o tratamento a ser realizado com vedação a tratamentos incompatíveis com as orientações do controlador. Assinar termos de confidencialidade (non-disclosure agreement - NDA) com os funcionários da empresa.
Controle de acesso	Implementar um sistema de controle de acesso aplicável a todos os usuários, com níveis de permissão na proporção da necessidade de trabalhar com o sistema e de acessar dados pessoais. Configurar funcionalidades no sistema de controle de acesso que possam detectar e não permitir o uso de senhas que não respeitem um certo nível de complexidade. Implementar um adequado gerenciamento de senhas, estabelecendo controles tais como: • evitar o uso de senhas padrão disponibilizadas pelos fornecedores de software ou hardware adquiridos; • utilizar apenas senhas complexas para acessar aplicativos e outros sistemas informáticos; • não reutilizar senhas. Proibir o compartilhamento de contas ou de senhas entre funcionários.

	Aplicar o princípio do menor privilégio (need to know). Utilizar a autenticação multi-fator para acessar sistemas ou base de dados que contenham dados pessoais. Implementar um sistema de controle de acesso aplicável a todos os usuários que acessam o sistema de TI (caso o agente de tratamento possua rede interna de computadores).
Segurança dos dados pessoais armazenados	Coletar e processar apenas os dados pessoais que são realmente necessários para atingir os objetivos do tratamento para a finalidade pretendida, minimizando a coleta de dados. Implementar soluções de pseudonimização, como a criptografia, para cifrar dados pessoais. Orientar os funcionários para não desativar ou ignorar as configurações de segurança de estações de trabalho. Evitar a transferência de dados pessoais de estações de trabalho para dispositivos de armazenamento externo, como pendrives e discos rígidos externos. Inventariar e cifrar dados de dispositivos externos e armazená-los em locais seguros. Realizar backups offline, periódicos e armazená-los de forma segura. Formatar e sobrescrever mídias físicas que contenham dados pessoais antes de descartá-las, ou, quando não for possível a sobrescrita, destruir as mídias físicas. Estabelecer no contrato de serviço o registro da destruição/descarte (caso o agente de tratamento utilize serviços de terceiros para o descarte).
Segurança das comunicações	Utilizar conexões cifradas (TLS/HTTPS) ou aplicativos com criptografia fim-a-fim para serviços de comunicação. Instalar e manter um sistema de firewall e/ou utilizar um Web Application Firewall (WAF – Filtro de Aplicação). Proteger e-mails via adoção de ferramentas AntiSpam, filtros de e-mail e, integrar o antivírus ao sistema de e-mail. Remover quaisquer dados sensíveis e outros dados pessoais que estejam desnecessariamente disponibilizados em redes públicas.
Gerenciamento de vulnerabilidades	Atualizar periodicamente todos os sistemas e aplicativos utilizados, mantendo os em sua versão atualizada (instalar patches de segurança disponibilizados pelos fornecedores). Adotar e atualizar periodicamente softwares antivírus e antimalwares. Realizar varreduras antivírus periódicas nos dispositivos e sistemas utilizados.
Dispositivos móveis	Utilizar técnicas de autenticação multi-fator para controle de acesso de dispositivos móveis – como smartphones e laptops. Separar os dispositivos móveis de uso privado daqueles de uso institucional, quando possível. Implementar funcionalidades que permitam apagar remotamente os dados pessoais armazenados em dispositivos móveis.

Serviços em nuvem	Realizar um contrato de acordo de nível de serviço com o provedor de serviços em nuvem, contemplando a segurança dos dados armazenados. Avaliar se o serviço oferecido pelo provedor do serviço em nuvem atende os demais requisitos de segurança da informação estabelecidos. Analisar os requisitos para o acesso do usuário a cada serviço em nuvem utilizado. Utilizar técnicas de autenticação multifator para acesso aos serviços em nuvem relacionados a dados pessoais.

ANPD. Guia Orientativo – Segurança da informação para agentes de tratamento de pequeno porte. 2021. p. 5. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf.

ANPD. Guia Orientativo – Segurança da informação para agentes de tratamento de pequeno porte. 2021. p. 5. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf.

Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/checklist-vf.pdf.

A adequação à LGPD é um esforço essencial para pequenas e médias empresas, garantindo a conformidade com a legislação e a proteção dos dados pessoais de clientes e colaboradores. Esse processo pode ser realizado de forma compatível com os recursos e a realidade de cada empresa, evitando custos excessivos. Assim, adotar práticas adequadas à LGPD não apenas cumpre uma obrigação legal, mas também contribui para a construção de confiança e segurança no relacionamento com os clientes.

8. DIREITO DOS TITULARES

Os direitos dos titulares previstos na LGPD garantem que as pessoas físicas tenham controle sobre seus próprios dados, em linha com o princípio da autodeterminação informacional. A responsabilidade de assegurar esses direitos recai sobre o controlador, que deve implementar mecanismos eficazes e transparentes para permitir o acesso, correção, exclusão, transferência, oposição ao tratamento e retirada de consentimento, entre outros. Contudo, essa responsabilidade pode ser compartilhada caso ajustado dessa forma entre as partes.

Entre os desafios que as empresas enfrentam para garantir esses direitos, destaca-se o desafio de criação de processos eficientes para atender às solicitações dos titulares. Além disso, a implementação de uma infraestrutura tecnológica adequada para assegurar a segurança, confidencialidade e disponibilidade dos dados exige um investimento significativo, especialmente para pequenas e médias empresas.

Na LGPD, os direitos estão previstos principalmente nos artigos 9º, 18, 20 e 23:

DIREITOS APLICÁVEIS EM QUALQUER CONTEXTO

- Confirmação da existência de tratamento (Art. 18, I): O titular pode solicitar a confirmação de que seus dados pessoais estão sendo tratados por determinada empresa.
- Acesso aos dados (Art. 18, II): Confirmada a existência do tratamento de dados, o titular terá o direito de acessar os dados pessoais que são tratados por determinada empresa.
- Correção dos dados (Art. 18, III): O titular pode solicitar a correção dos dados incompletos, incorretos e/ou desatualizados.
- Informações sobre compartilhamento (Art. 18, VII): O titular pode solicitar informações sobre as entidades públicas e privadas com as quais a empresa realiza uso compartilhado de dados.
- Portabilidade (Art. 18, V e § 7º): O titular pode solicitar a portabilidade dos seus dados para outro fornecedor de serviço ou produto, observados os segredos comercial e industrial. Essa portabilidade não inclui dados que já tenham sido anonimizados pelo controlador.

DIREITOS APLICÁVEIS QUANDO HOUVER TRATAMENTO EM DESCONFORMIDADE COM A LGPD

- Anonimização, bloqueio ou eliminação (Art. 18, IV): O titular pode solicitar a anonimização, bloqueio e eliminação de dados desnecessários, excessivos e/ou tratados em desconformidade com a LGPD.
- Oposição (Art. 18, § 2º): O titular pode opor-se ao tratamento realizado com fundamento em uma Anonimização, bloqueio ou eliminação (Art. 18, IV): O titular pode solicitar a anonimização, bloqueio e eliminação de dados desnecessários, excessivos e/ou tratados em desconformidade com a LGPD.
- Oposição (Art. 18, § 2º): O titular pode opor-se ao tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento à LGPD.

DIREITOS APLICÁVEIS QUANDO A BASE LEGAL FOR CONSENTIMENTO

- Eliminação de dados (Art. 18, VI): O titular pode solicitar a eliminação de dados tratados com base no consentimento, exceto nas hipóteses de conservação dos dados após o término do seu tratamento previstas no Art. 16 da LGPD, quais sejam: (i) cumprimento de obrigação legal ou regulatória pelo controlador; (ii) estudo por órgão de pesquisa, garantida a anonimização dos dados; (iii) transferência a terceiro; ou (iv) uso exclusivo do controlador, vedado o acesso por terceiro, e desde que anonimizados os dados.
- Possibilidade de não fornecer o consentimento (Art. 18, VIII): O titular deverá ser informado sobre a possibilidade de não fornecer consentimento e as consequências dessa negativa.
- Revogação do consentimento (Art. 8º, § 5º e Art. 18, IX): O titular tem o direito de revogar o consentimento a qualquer momento por meio de procedimento gratuito e simplificado. Caso isso ocorra, ficam ratificados eventuais tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação (Art. 18, VI).

DIREITOS APLICÁVEIS EM FACE DE **DECISÕES AUTOMATIZADAS**

- Revisão da decisão (Art. 20, caput): O titular tem o direito de solicitar revisão das decisões tomadas exclusivamente com base em tratamento automatizado de dados que afetem os seus interesses, como decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
- Critérios da decisão (Art. 20, § 1º): O titular pode obter informações claras e adequadas sobre os critérios e procedimentos utilizados para as decisões automatizadas, sempre observado os segredos comercial e industrial.

As empresas podem ser proativas no atendimento aos direitos dos titulares, especialmente os previstos no Art. 9º da LGPD, que exigem que as informações sejam de fácil acesso.

Em geral, o requerimento do titular para o exercício dos direitos descritos no Art. 18 da LGPD deve ser gratuito. Para facilitar a comunicação entre titulares e os responsáveis pelo tratamento, as empresas podem fornecer formulários, físicos ou on-line, que incluam as principais informações necessárias para a análise do pedido, além de comprovar a identidade do titular e a viabilidade da requisição. Entre as informações que podem ser solicitadas estão:

Identificação da categoria do titular: se cliente; ex-cliente; fornecedor ou terceiro; funcionário ou colaborador; outros.

Seleção do tipo de solicitação: com a indicação dos direitos previstos na LGPD.

Detalhes da solicitação: com espaço para descrição subjetiva do titular.

Dados de identificação: como e-mail; nome completo; telefone; envio da cópia de documento de identificação, a exemplo do CPF ou RG.

Para comprovar a identidade do titular, a instituição deve estabelecer condições razoáveis que garantam a confirmação de quem está solicitando o direito. O nível de autenticação pode variar conforme a sensibilidade da solicitação, e a empresa deve assegurar que o compartilhamento de documentos seja realizado de forma segura, exclusivamente para essa finalidade.

No que diz respeito à confirmação da existência ou ao acesso aos dados, o artigo 19 da LGPD orienta que o titular pode solicitar informações que devem ser fornecidas de forma imediata e simplificada (Art. 19, I) ou, em até quinze dias, através de uma declaração clara e completa. Essa declaração deve indicar a origem dos dados, a inexistência de registros, os critérios utilizados e a finalidade do tratamento, respeitando os segredos comercial e industrial (Art. 19, II). O parágrafo 4º do artigo 19 permite que prazos diferentes sejam aplicados para setores específicos, conforme decisão da ANPD.

As informações e os dados a serem compartilhados podem ser fornecidos eletronicamente, por um meio "seguro e adequado" (Art. 19, §2º, I), ou impressos (Art. 19, §2º, II), conforme a preferência do titular. Além disso, os dados devem ser armazenados em formatos que facilitem o exercício do direito de acesso.

Portanto, a LGPD exige que as ações dos agentes de tratamento sejam desenvolvidas para garantir efetivamente o controle dos dados pelos titulares. Isso inclui organizar fluxos internos que permitam identificar e responder com precisão às solicitações, além de assegurar a segurança tecnológica no armazenamento, compartilhamento e exclusão de dados.

RECOMENDAÇÕES PARA **ATENDIMENTO AOS DIREITOS DOS TITULARES**

- Disponibilize meio adequado para os titulares enviarem seus requerimentos, seja por e-mail, formulário, portal ou outro canal de comunicação disponível.
- Monitore todos os canais de comunicação disponíveis aos titulares para que seja possível cumprir os prazos legais de resposta.
- Confirme se a pessoa que está exercendo os seus direitos é o titular daqueles dados para evitar que terceiros tenham acesso a essas informações.
- Atualize regularmente as formas de contato com o controlador e o encarregado, em páginas eletrônicas ou avisos físicos, indicando o nome e e-mail do responsável.
- Caso o agente de tratamento de pequeno porte opte por não indicar um encarregado, ele deve disponibilizar um canal de comunicação com o titular, com pelo menos duas opções de contato, como e-mail e formulário.
- Forneça as informações sobre o tratamento de dados de forma concisa, transparente, clara e acessível.
- Utilize uma linguagem simplificada e acessível ao comunicar-se com o titular, evitando jargões jurídicos.
- Quando não for possível atender a um pedido, forneça uma justificativa legal clara.
- Mantenha atualizados os documentos necessários para a conformidade com a proteção de dados, como o mapeamento de dados (data mapping), que identifica quais dados são tratados e como.
- Revise contratos, especialmente com parceiros que atuem como operadores de dados, prevendo a comunicação e as responsabilidades no atendimento aos direitos dos titulares.
- Desenvolva fluxos internos para o atendimento das requisições dos titulares, definindo prazos e responsáveis.
- Registre todas as providências tomadas e informações analisadas ao responder às requisições dos titulares. Isso não só demonstra conformidade com a LGPD, mas também facilita a defesa em caso de questionamentos ou auditorias.
- As informações devem ser disponibilizadas em português, de forma simples e intuitiva, facilitando a navegação do usuário.
- Evite o excesso de informações, e utilize fontes, cores e elementos visuais que tornem o conteúdo acessível, destacando as informações mais importantes.

Caso o pedido seja de correção, eliminação, anonimização ou bloqueio dos dados, e for possível adotar as providências solicitadas, o controlador deve, de maneira imediata, informar os agentes de tratamento com quem tenha realizado uso compartilhado dos dados para que eles repitam o procedimento idêntico, exceto se esta comunicação for comprovadamente impossível ou implicar em esforço desproporcional (Art. 18, §6º).

Ao analisar as requisições dos titulares, os agentes de tratamento podem identificar limitações que impedem o atendimento, como nos casos em que a empresa não é a responsável pela solicitação. Nesses casos, o titular deve ser informado sobre os motivos pelos quais o pedido não pode ser atendido, parcial ou totalmente, com a devida explicação dos fatos ou fundamentos legais que inviabilizam o atendimento (Art. 18, §4º, da LGPD). Além disso, quando aplicável, o titular deve ser orientado sobre quem são os agentes de tratamento responsáveis e receber informações sobre possíveis alternativas.

Vale destacar que no caso do não atendimento de uma requisição do titular de dados em relação aos seus direitos, ou no caso em que a resposta não for adequada, o titular poderá recorrer à ANPD ou mesmo ao Poder Judiciário para procurar obter a satisfação de sua demanda. Por isso, garantir os direitos dos titulares é essencial para cumprir a legislação da proteção de dados.

9. RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é uma "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (Art. 5º, XVII, da LGPD).

O RIPD deve ser elaborado e mantido pelo controlador, conforme previsto nos artigos 5º, inciso XVII, e 38, da LGPD, e, como regra geral, deve ser encaminhado à ANPD quando solicitado pela Autoridade*, o que pode ocorrer a qualquer momento (Arts. 32 e 38, da LGPD). Esta possibilidade reforça o cuidado que os agentes de tratamento devem ter antes de iniciar determinados tratamentos de dados pessoais, bem como prosseguirem com o processo de adequação à ANPD e aperfeiçoamento de suas estratégias.

Para o setor de saúde, é possível indicar os exemplos abaixo como hipóteses que exigem a elaboração do RIPD. É importante ressaltar que a avaliação da necessidade deve ocorrer conforme cada caso, sob a responsabilidade do controlador.

* ANPD. Relatório de Impacto à Proteção de Dados Pessoais (RIPD). 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p4.

EXEMPLOS DE HIPÓTESES PARA **ELABORAÇÃO DO RIPD**

- Para uso de ferramentas de identificação pessoal que utilizem dados pessoais sensíveis ou sejam invasivos (como reconhecimento facial) para controle de acesso e prevenção à fraude.
- Para adoção de novas tecnologias, como novos aplicativos e modalidades de telessaúde por prestadores de serviços de saúde.
- Para o tratamento automatizado de dados e análise de perfis, com o objetivo de prestação de serviços de corretagem.
- Para monitoramento do uso de dispositivos médicos, no caso de fornecedores e distribuidores acompanharem o uso de equipamentos ou dispositivos médicos em tempo real (por exemplo, dispositivos IoT na área da saúde).

Conforme as orientações emitidas pela ANPD, o RIPD será necessário quando se verificar que o tratamento a ser realizado poder implicar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados.

COMO IDENTIFICAR QUE UM **TRATAMENTO É DE ALTO RISCO**?

Critérios Gerais:

- Há tratamento de dados pessoais em larga escala?
- Há tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares?

Critérios Específicos:

- Há uso de tecnologias emergentes e inovadoras?
- Há vigilância e controle de zonas acessíveis ao público?
- São tomadas decisões unicamente com base em tratamento automatizado de dados pessoais?
- Há uso de dados pessoais sensíveis, dados pessoais de crianças, de adolescentes ou de idosos?

PONTOS DE **ATENÇÃO**

1. Por tratamento de larga escala deve-se considerar todo tratamento que abranger número de titulares e volume de dados significativo (Segundo a ANPD, igual o maior a 2 milhões de pessoas), bem como a duração, a frequência e a extensão geográfica.
2. O prejuízo aos direitos fundamentais será caracterizado quando o tratamento puder impedir o exercício de direitos ou a utilização de um serviço, ou causar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.
3. Conforme disposto na Resolução CD/ANPD nº 2/2022, é de responsabilidade do agente de tratamento comprovar, quando solicitado pela ANPD, que se enquadra nas disposições do Art. 2º (com as definições para agentes de tratamento de pequeno porte, microempresas e empresas de pequeno porte e startups) e do Art. 3º (requisitos para se beneficiar do tratamento jurídico diferenciado previsto no Regulamento) em até quinze dias.

ANPD. Guia Orientativo Tratamento de Dados Pessoais de Alto Risco. 2024. Disponível em: https://www.gov.br/participamaisbrasil/estudopreliminar-altorisco?utm_campaign=governanca_de_dados_anpd_cp_alto_risco&utm_medium=email&utm_source=RD+Station

O controlador pode optar por elaborar um único RIPD que abranja as operações de tratamento com a mesma finalidade ou criar um RIPD específico para cada operação. A recomendação depende do contexto. Quando as operações de tratamento são distintas entre si, é recomendável que sejam elaborados relatórios separados para facilitar a identificação dos tratamentos realizados e dos riscos associados.

Por outro lado, se as operações de tratamento forem similares em natureza, finalidade e riscos, um único RIPD pode ser suficiente para englobar todas essas operações. Além disso, é importante lembrar que, em casos de compartilhamento de dados pessoais entre diferentes controladores, cada um poderá ser responsável por seu próprio RIPD, mesmo que usem uma plataforma compartilhada, já que as finalidades do tratamento podem variar.

1. *O parágrafo único do artigo 38 da LGPD também define que o RIPD deve conter minimamente:*
2. *a descrição dos tipos de dados pessoais coletados ou tratados de qualquer forma;*
3. *a metodologia usada para o tratamento e para a garantia da segurança das informações; e*
4. *a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados.*

Além disso, a ANPD disponibiliza as seguintes recomendações quanto ao conteúdo do RIPD:

INFORMAÇÕES RECOMENDADAS **PELA ANPD PARA INCLUSÃO NO RIPD**

- Identificação dos agentes de tratamento e do encarregado;
- Outras partes interessadas/envolvidas. Informar se foram consultadas na elaboração do RIPD e pareceres emitidos;
- Justificativa da necessidade de elaboração do relatório (por exemplo: alto risco, solicitação da ANPD, gestão de riscos e prevenção, outros);
- Projeto/Processo que justifica a elaboração do RIPD;
- Sistemas de informação relacionados ao projeto/processo que justifica a elaboração do RIPD;
- Tratamento de dados;

1. Descrição do tratamento (desde a coleta até a eliminação);
2. Dados pessoais (informar todos os tipos de dados pessoais tratados, de forma completa);
3. Dados pessoais sensíveis (informar todos os tipos de dados pessoais sensíveis tratados, de forma completa);
4. Categorias de titulares (por exemplo, clientes, funcionários do controlador, filhos de funcionários do controlador, funcionários de clientes, autores de ações judiciais, beneficiários de apólices, terceiros prestadores de serviços);
5. Dados de crianças e adolescentes ou de outra categoria de vulneráveis, como idosos, se houver;
6. Volume de dados pessoais tratados e número de titulares envolvidos no tratamento;
7. Fonte de coleta;
8. Finalidade do tratamento (Justifique a finalidade de tratamento para cada dado);
9. Informar quais são os compartilhamentos internos e externos (inclusive transferência internacional, se houver);
10. Política de armazenamento (descrever os prazos de retenção e métodos de descarte).

- Análise de hipótese legal. Justifique a escolha da hipótese legal para cada finalidade de tratamento;
- Análise de princípios da LGPD;
- Riscos identificados ao titular;
- Resultado apurado com base na metodologia utilizada pelo agente de tratamento:
- Descrição do risco e do impacto para os titulares;
- Portabilidade;
- Impacto;
- Risco total.

11. Medidas, salvaguardas e mecanismos de mitigação de risco:

- Risco;
- Tratamento de risco, com descrição das medidas adotadas para mitigação do risco;
- Risco após o tratamento;
- Risco residual.
- Comentários e aprovações.

O controlador pode avaliar se cabe a inclusão de informações complementares ao indicado acima. Além disso, a própria ANPD também pode solicitar informações adicionais sobre o RIPD, quando assim entender necessário (Art. 38, da LGPD).

Ainda, quando o tratamento for realizado de acordo com a base legal do legítimo interesse é possível que o RIPD seja solicitado pela Autoridade (Art. 10, §3°, da LGPD).

ANPD. Relatório de Impacto à Proteção de Dados Pessoais (RIPD). 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p8. ANPD. Relatório de Impacto à Proteção de Dados Pessoais (RIPD). 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p12.

Para auxiliar os controladores, apresenta-se a seguir a sugestão indicada pela ANPD quanto às fases de elaboração do RIPD:

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Identifique os agentes de tratamento e o encarregado.

Identifique outras partes interessadas/envolvidas.

Avalie a justificativa da necessidade de elaborar ou atualizar o relatório.

Caso seja necessário elaborar ou atualizar o RIPD

Descreva o tratamento de dados.

Analise a base legal.

Analise os princípios da LGPD.

Avalie os riscos identificados.

Estabeleça medidas, salvaguardas e mecanismos de mitigação de risco.

Colete comentários e aprovações.

Monitore a aplicação do RIPD e atualize o documento e procedimentos adotados, se necessário.

Quanto à descrição do tratamento de dados, é necessário identificar as operações realizadas, os tipos de dados envolvidos e a categoria dos titulares (por exemplo, se são clientes ou colaboradores de um determinado grupo da instituição). Assim, é fundamental analisar a natureza, o escopo, o contexto e a finalidade do tratamento, com o objetivo de obter os subsídios necessários para a avaliação e a gestão de riscos, de acordo com a realidade da organização:

ANPD. Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd.

BRASIL. Guia de Boas Práticas para Implementação da Lei Geral de Proteção de Dados na Administração Pública Federal. 2020, p. 35-36. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf.

ELEMENTOS PARA A **DESCRIÇÃO DO TRATAMENTO**

Natureza

- Avaliação de como a organização trata ou pretender tratar determinado dado pessoal. A descrição pode incluir:
- como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados.
- fonte de dados (ex: titular de dados, planilha eletrônica, arquivo xml, formulário em papel, etc.) utilizada para coleta dos dados pessoais.
- com quais órgãos, entidades ou empresas os dados pessoais serão compartilhados.
- quais são os operadores que realizam o tratamento de dados pessoais em nome do controlador e destacar em quais fases (coleta, retenção, processamento, compartilhamento, eliminação) eles atuam.
- se adotou recentemente algum tipo de nova tecnologia ou método de tratamento que envolva dados pessoais. A informação sobre o uso de nova tecnologia ou método de tratamento é importante no sentido de possibilitar a identificação de possíveis riscos resultantes de tal uso.
- medidas de segurança atualmente adotadas

Escopo

- Avaliação da abrangência do tratamento de dados. A descrição pode incluir:
- as informações sobre os tipos dos dados pessoais tratados, ressaltando quais dos dados são considerados dados pessoais sensíveis.
- o volume dos dados pessoais a serem coletados e tratados.
- a extensão e frequência em que os dados são tratados.
- o período de retenção, informação sobre quanto tempo os dados pessoais serão mantidos, retidos ou armazenados.
- o número de titulares de dados afetados pelo tratamento.
- a abrangência da área geográfica do tratamento.

Contexto

- Análise ampla sobre fatores internos e externos que podem afetar as expectativas e a boa-fé do titular de dados ou sobre o tratamento. A descrição pode incluir:
- natureza do relacionamento da organização com os indivíduos.
- nível ou método de controle que os indivíduos exercem sobre os dados pessoais.
- destacar se o tratamento envolve crianças, adolescentes ou outro grupo vulnerável.
- destacar se o tipo de tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais. Ou seja, o dado pessoal não é tratado de maneira diversa do que é determinado em leis e regulamentos, e comunicado pela instituição ao titular de dados.
- destaque de qualquer experiência anterior com esse tipo de tratamento de dados.
- destaque de avanços relevantes da instituição em tecnologia ou segurança que contribuem para a proteção dos dados pessoais.

Finalidade

- Análise da definição da finalidade pela qual o dado é ou será tratado. A descrição pode incluir a avaliação sobre o embasamento legal pelo qual o dado é tratado, com avaliação dos artigos 7° e 11 da LGPD, quando aplicável. Além disso, é recomendável:
- Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais, informando o quão importantes são esses resultados.
- Informar os benefícios esperados para o órgão, entidade ou para a sociedade como um todo.

Em relação à análise das condições de legitimidade de tratamento de dados, com a avaliação sobre a proporcionalidade e legalidade do tratamento conforme as garantias dos titulares de dados. Os princípios da finalidade, adequação e necessidade devem orientar a avaliação para que o tratamento ocorra apenas sobre o mínimo necessário para atender a finalidade específica pretendida.

AVALIAÇÃO DAS CONDIÇÕES DE LEGITIMIDADE DO TRATAMENTO

- Analise a fundamentação legal para o tratamento dos dados pessoais.
- Caso o fundamento legal seja embasado no legítimo interesse do controlador (LGPD, Art. 10), deve-se demonstrar que:
- esse tratamento de dados pessoais é indispensável;
- não há outra base legal possível de se utilizar para alcançar o mesmo propósito; e
- esse processamento de fato auxilia no propósito almejado.
- Indique como será garantida a qualidade (exatidão, clareza, relevância e atualização dos dados) e minimização dos dados.
- Demonstre quais medidas são adotadas a fim de assegurar que o operador (LGPD, Art. 5º, VII) realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador (LGPD, Art. 5º, VI).
- Registre como estão implementadas as medidas que asseguram o direito do titular dos dados pessoais obter do controlador o previsto pelo Art. 18 da LGPD.

- Explique como a instituição pretende fornecer informações de privacidade para os titulares dos dados pessoais.
- Sinalize quais são as salvaguardas em casos de transferências internacionais de dados.

A análise das condições de legitimidade do tratamento de dados pode contribuir para a identificação de riscos, sejam eles existentes ou potenciais. Nesse processo, podem ser utilizados parâmetros como a matriz probabilidade x impacto sobre a proteção de dados, além de padrões de certificação.

Para a mitigação de riscos, devem ser desenvolvidas ações de segurança, 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 qualquer forma de tratamento inadequado ou ilícito" (Art. 46, LGPD).

O RIPD pode ser submetido à análise para coleta de comentários, consultando "partes interessadas relevantes, internas e externas", que ofereçam opiniões legais, técnicas ou administrativas sobre o tratamento de dados. É recomendável identificar as partes consultadas e as recomendações feitas sobre o tratamento e os riscos envolvidos.

A aprovação do RIPD é fundamental para sua formalização, com a obtenção das assinaturas dos responsáveis pela sua elaboração, do encarregado e das autoridades que representam o controlador e o operador.

Após a aprovação, o RIPD deve ser monitorado e atualizado periodicamente, seja anualmente ou diante de qualquer mudança que afete o tratamento de dados pessoais na instituição. Manter o Relatório de Impacto à Proteção de Dados em constante revisão é essencial para garantir uma avaliação contínua dos riscos, considerando as transformações nos cenários tecnológico, normativo e institucional, o que é crucial para a modernização e competitividade das empresas.

A respeito, orienta-se que "caso não seja conveniente registrar o que foi consultado, então é importante apresentar o motivo de não ter realizado tal registro. Como, por exemplo, apresentar justificativa de que informar o registro das opiniões das partes internas comprometeria segredo comercial ou industrial; fragilizaria a segurança da informação; ou seria desproporcional ou impraticável realizar o registro das opiniões obtidas." (BRASIL. Guia de Boas Práticas para Implementação da Lei Geral de Proteção de Dados na Administração Pública Federal. 2020, p. 38. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.

BRASIL. Guia de Boas Práticas para Implementação da Lei Geral de Proteção de Dados na Administração Pública Federal. 2020, p. 42. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. pdf).

10. CRIAÇÃO DE UMA CULTURA DE PROTEÇÃO DE DADOS PESSOAIS

Uma cultura de proteção de dados pessoais pode ser entendida como o padrão de conhecimento e comportamento adotado por determinada instituição, capaz de ser orientado através da governança corporativa, com adoção de políticas internas e capacitação dos funcionários.

Ao falar em cultura de proteção de dados pessoais, o que está em debate é o comportamento das pessoas da organização. Incentivar a cultura de privacidade nas instituições garante que as pessoas entendam e sigam as práticas recomendadas para redução de riscos, uma vez que, na prática, são as responsáveis pelas ações internamente.

A adoção de um programa de privacidade permite a mudança de cultura organizacional das empresas. O programa deve ser personalizado para atender às necessidades e requisitos específicos de uma empresa, considerando os tipos de dados pessoais coletados, os fins para os quais são utilizados e as normas legais e regulatórias aplicáveis.

Neste programa, é possível identificar os grupos que tratam diretamente com dados pessoais, em especial, os sensíveis, e que em razão disso precisem de ações mais específicas em razão de seu trabalho abranger o tratamento significativo de dados pessoais. Como exemplos de grupos que exigem maior atenção, pode-se indicar as equipes das áreas da alta direção, segurança da informação, recursos humanos e canais de atendimento, como os Serviços de Atendimento ao Consumidor (SAC) e ouvidoria, além da equipe de marketing.

Ademais, o programa de privacidade deve ser revisado e atualizado periodicamente para garantir sua relevância e eficácia contínuas, protegendo a confiança de clientes com as ações da empresa já que cada vez mais estão preocupados com sua privacidade e segurança de seus dados.

Além de ações para grupos específicos de colaboradores, é necessário que todos da organização sejam capacitados quanto às melhores práticas para proteção de dados pessoais. O treinamento é uma ferramenta essencial para que os prestadores de serviços de saúde garantam que os membros da equipe estejam em conformidade e totalmente capacitados sobre a responsabilidade que têm em relação aos dados pessoais dos pacientes e à proteção dessas informações.

AÇÕES PARA CONSCIENTIZAÇÃO SOBRE **PROTEÇÃO DE DADOS PESSOAIS**

- Incentive a capacitação de funcionários, por meio de cursos internos ou externos, presenciais ou remotos.
- Desenvolva ações de endomarketing para engajar e orientar as equipes sobre as melhores práticas de proteção de dados e segurança da informação.
- Estabeleça cronogramas de treinamento que incluam palestras, vídeos e informações atualizadas sobre proteção de dados pessoais.
- Promova a capacitação de novos funcionários sobre as normas da instituição e crie mecanismos que comprovem a participação e compreensão do treinamento, como certificados ou declarações.
- Elabore materiais internos, como cartilhas sobre temas específicos. Este guia de orientações sobre a LGPD no setor de saúde pode ser uma fonte relevante para seus colaboradores.
- Alinhe os documentos institucionais, como missão e visão organizacional, para que a promoção da cultura de privacidade seja integrada aos objetivos da instituição.
- Inclua a privacidade como parâmetro nos processos internos de orientação e treinamento de novos funcionários.

No caso de consultórios e demais empreendimentos que prestam serviços de saúde, por exemplo, é importante que todo o pessoal da organização, clínico e não clínico, tenha competência técnica no uso de sistemas clínicos e nos serviços oferecidos pelo sistema.

A depender do público-alvo, é possível que as campanhas de orientação envolvam parceiros contratuais e clientes, com o fornecimento de materiais explicativos sobre conceitos básicos da proteção de dados e eventuais atualizações adotadas pela organização.

As instituições podem desenvolver ações de benchmarking, para identificação e análise das melhores práticas de gestão de uma organização, com o objetivo de melhorar o desempenho da própria empresa. A troca de experiências sobre as condutas que devem ser adotadas para capacitação em proteção de dados pessoais podem estimular a criatividade e o desenvolvimento de novas soluções que estejam em conformidade com a LGPD e demais normas reguladoras.

A LGPD incentiva em seu artigo 50 que os controladores e operadores, no âmbito de suas competências, possam formular regras de boas práticas e de governança para o tratamento de dados pessoais, individualmente ou por meio de associações. Exemplos de boas iniciativas que objetivam desenvolver o diálogo entre o setor é a do Fórum Permanente do Setor de Saúde em Proteção de Dados e Privacidade, cujo presente documento é resultado desse esforço em buscar diálogo e construir melhores compreensões e práticas sobre a proteção de dados no setor econômico.

Diante do investimento das organizações para desenvolver a cultura de proteção de dados pessoais, também é válido implementar medidas que visem a avaliar a qualidade da cultura adotada. Isso pode ser feito através da avaliação de solicitações de aspectos como a capacidade de respostas às solicitações dos titulares, com análise do tempo e qualidade da providência adotada por seus colaboradores.

A partir da experiência internacional, é possível criar funções conhecidas como "Embaixadores da Privacidade" ou "Defensores da Privacidade", com a indicação de funcionários de destaque que podem contribuir com a promoção de boas práticas em proteção de dados. Vale frisar que não se trata de um cargo ou espécie de agente de tratamento prevista na LGPD ou pela ANPD.

Para as ações que podem ser desenvolvidas para a criação de uma cultura de proteção de dados pessoais nas instituições, o papel do encarregado de dados possui o destaque para auxiliá-las, porque deve agir na orientação dos funcionários e os contratados da organização sobre as práticas a serem tomadas em relação à proteção de dados pessoais e demais orientações definidas pelo controlador (Art. 41, §2º, III e IV, da LGPD).

As ações para a promoção da cultura de privacidade devem considerar a realidade de cada instituição, a qual precisa atuar para identificar o seu estado atual, vulnerabilidades, oportunidades de melhoria e prioridades. Por isso a importância do engajamento da direção executiva, que poderá coordenar as ações com os demais colaboradores para construir e manter uma cultura de conscientização sobre privacidade.

11. SEGURANÇA DA INFORMAÇÃO

No setor de saúde, os desafios para a garantia da segurança da informação merecem atenção diante da grande quantidade de dados tratados, a tendência de maior uso de dados sensíveis (especialmente os dados de saúde), e a intrincada rede de serviços e atores público-privados. Garantir a segurança da informação significa desenvolver ações para a "preservação da confidencialidade, integridade e disponibilidade da informação", essencial para a confiança nos negócios e proteção de direitos.

A LGPD exige a adoção de medidas de segurança da informação para garantia da segurança dos dados pessoais, as quais devem ser técnicas ou administrativas, de forma preventiva e reativa. Além disso, devem abranger a concepção de serviços e produtos, a sua execução e todo o ciclo de vida dos dados – conforme os princípios privacy by design e privacy by default.

O pilar da arquitetura tecnológica da ANPD inclui medidas para promoção da proteção de dados pessoais inclusive nos meios digitais, indicando-se inicialmente no artigo 6º, VII, da LGPD, com o princípio da segurança e nas determinações dos artigos 46 a 49 da Lei. De acordo com o Art. 46 da LGPD, as ações para a segurança da informação devem ser capazes de 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.

Além disso, a Lei define em seu Art. 49 que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados para também atender aos padrões de boas práticas e de governança, bem como os princípios gerais previstos na LGPD e demais normas. Destaca-se que obrigação de garantir a segurança da informação estende-se a qualquer outra pessoa que intervenha em uma das fases do processamento de dados, mesmo após o seu término (Art. 47 da LGPD), não limitando-se, portanto, apenas aos agentes de tratamento.

A relevância do tema não se restringe ao Brasil. Pela primeira vez, em 2023, a Agência da União Europeia para Segurança Cibernética (ENISA) publicou uma análise sobre o cenário de ameaças cibernéticas no setor de saúde e identificou que os incidentes de segurança na União Europeia envolveram, principalmente, violações ou roubo de dados e a interrupção de serviços de saúde.

AMEAÇAS **CIBERNÉTICAS** NO SETOR DE SAÚDE NA UE

O relatório da ENISA destacou ataques direcionados a dispositivos inteligentes, como dispositivos vestíveis (wearables) e equipamentos médicos, como umas das principais preocupações a nível de segurança da informação para empresas no setor de saúde. Essa invasão pode afetar todos os tipos de dispositivos médicos utilizados para cuidados a idosos, cuidados domiciliários, cuidados de saúde mental e cuidados a deficientes, tais como botões de emergência e tecnologias de monitoramento remoto (RMT). Se tais dispositivos forem explorados ou bloqueados, a segurança dos pacientes e, em alguns casos, a segurança dos profissionais de saúde pode estar em risco.

Diante dessas ameaças, a ENISA recomenda que as empresas do setor tenham um programa dedicado de defesa contra ransomware, tenham um programa de conscientização de segurança para equipes não relacionadas a tecnologia da informação, realizem avaliações de risco, e realizem avaliações regulares de vulnerabilidades para identificar e resolver uma brecha de segurança, especialmente em dispositivos voltados para a Internet. Essas ações visam para limitar a superfície que pode ser atacada por agentes maliciosos.

Os incidentes envolvendo dados pessoais podem favorecer a ocorrência de fraudes e facilitar que outras espécies de crimes ocorram. Além disso, trata-se de incidentes mais graves, já que envolvem normalmente a exposição de dados sensíveis, com alto potencial de colocar os titulares de dados em situações de exposição, violando a sua privacidade.

Os riscos com incidentes de segurança podem ser bastante elevados, afetando não apenas os titulares de dados, mas também a reputação das empresas e responsáveis, podendo acarretar prejuízos financeiros e perdas de oportunidades. Caso um tratamento indevido também envolva dados pessoais sensíveis, como os dados de saúde, há também um risco desses dados serem utilizados para fins discriminatórios e ilícitos, representando grave violação aos direitos dos titulares.

Para além de incidentes de segurança e de tratamento indevidos, os casos de fraude também devem ser destacados. Agentes fraudulentos podem utilizar de dados de saúde para diversos

tipos de ataque, inclusive em casos sofisticados com o uso de IA, a exemplo da criação de áudio, vídeo e texto falsos com base em informações de saúde, o que gera impacto no setor e demanda constante aperfeiçoamento e coordenação estratégica para adoção das melhores práticas.

Portanto, é importante que a estratégia de segurança da informação adotada seja abrangente e multidisciplinar, uma vez que a confidencialidade dos dados de saúde e a segurança da informação são relevantes para um ambiente de saúde seguro. As estratégias da segurança da informação no setor da saúde devem estar pautadas por ao menos em três aspectos: a) confidencialidade, para que o acesso de sistemas e dados ocorra apenas por usuários autorizados; b) integridade, para que os dados e sistemas sejam precisos e confiáveis; c) acessibilidade, para sistemas e dados quando solicitados.

COMUNICAÇÃO DE **INCIDENTE DE SEGURANÇA**

A Resolução CD/ANPD nº 15, de 24 de abril de 2024, regulamenta os casos e a forma de Comunicação de Incidente de Segurança para a ANPD. O regulamento apresenta a atuação da ANPD, especialmente o seu braço fiscalizatório, quando em face de incidentes de segurança. Em suma, a ANPD possui duas formas de atuação: (i) comunicação de incidente de segurança, quando o agente informa o incidente, ou (ii) apuração de incidente de segurança, ou seja, quando a autoridade por conta própria passa a apurar a ocorrência de incidentes que possam acarretar risco ou dano relevante aos titulares, não comunicados pelo controlador, de que venha a tomar conhecimento.

O procedimento de comunicação de incidente de segurança se inicia após o recebimento da comunicação do incidente pela ANPD. Essa comunicação é resultado de uma obrigação legal em que o agente de tratamento deve comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. O regulamento determina com maior precisão os critérios e parâmetros para a devida comunicação nos casos de incidente de segurança.

Dentre as principais ameaças à segurança da informação, é possível indicar:

EXEMPLOS DAS **PRINCIPAIS AMEAÇAS** À SEGURANÇA DA INFORMAÇÃO

Malwares	Formas de software de computador malicioso projetado para danificar ou comprometer sistemas e dispositivos. Exemplos incluem vírus, worms, ransomware e spyware, que podem roubar dados, criptografar arquivos ou permitir o controle remoto de sistemas infectados e geralmente são compartilhados via e-mail.
Ransomware	Exemplo de malware que criptografa os dados da vítima, exigindo um pagamento (resgate) para restaurar o acesso. Esse tipo de ataque pode paralisar operações de empresas e serviços essenciais.
Phishing	Quando um invasor envia uma mensagem fraudulenta para induzir uma pessoa a revelar informações confidenciais ou instalar malware no computador da vítima. Geralmente, envolve e-mails ou mensagens que parecem vir de fontes confiáveis.
Smishing	É uma variação do phishing que utiliza as mensagens de texto (SMS) como meio para enganar as vítimas, as induzindo para realizar uma ação específica, como clicar em um link malicioso ou divulgar informações.
Spoofing	Tipo de ataque cibernético em que um indivíduo ou programa se disfarça como outra pessoa ou entidade confiável para obter uma vantagem ilegítima. Normalmente ocorre através do envio de e-mails um endereço de remetente falsificado, mas existem outras variações como o caller ID spoofing, em que há a falsificação do número de telefone que aparece no identificador de chamadas; o website spoofing, com a criação de sites falsos imitando páginas legítimas para capturar informações pessoais; e o application spoofing, em que há o disfarce de um aplicativo legítimo para executar ações maliciosas.

Roubo e exfiltração de dados	Criminosos podem acessar, copiar e transferir dados confidenciais de uma organização, resultando em perda de propriedade intelectual, dados de clientes ou informações sensíveis.
Ataques DDoS (Distributed Denial of Service)	Criminosos podem acessar, copiar e transferir dados confidenciais de uma organização, resultando em perda de propriedade intelectual, dados de clientes ou informações sensíveis.

NHS England. Cyber Security. 2023. Disponível em: https://www.england.nhs.uk/long-read/cyber-security/.

As organizações podem atuar em diferentes frentes, como administrativamente, através da adoção de mecanismos para segurança das ferramentas tecnológicas e integridade das informações e por meio da conscientização e treinamento das pessoas. A abordagem conhecida como Security by Design pode orientar as organizações neste sentido, através da avaliação da vulnerabilidade, dos riscos aos quais a empresa é particularmente sensível, com análise da ferramenta de supervisão e sua capacidade de detectar, qualificar e notificar uma violação.

Ademais, é possível aumentar a conscientização entre as equipes de desenvolvedores de aplicativos e serviços, para que a criação e revisão de procedimentos considerem boas práticas de proteção de dados pessoais e segurança da informação. Para tanto, as organizações precisam saber quais de seus funcionários, clientes e fornecedores criam os dados em seu sistema de Tecnologia da Informação, bem como possuem acesso a dados e a aplicativos.

Administrativamente, as empresas devem atuar para estabelecer a estrutura e os processos na proteção da segurança da informação, em complemento às medidas técnicas e físicas, com a devida adequação legal.

MEDIDAS ADMINISTRATIVAS PARA **A SEGURANÇA DA INFORMAÇÃO**

- Invista em um programa de gerenciamento de riscos e avalie regularmente seus sistemas e práticas. Isso pode integrar as ações de compliance para adequação à LGPD.
- Desenvolva uma Política de Segurança da Informação (PSI) com diretrizes claras para proteger a instituição, especificando objetivos, alcance e responsabilidades.
- A PSI deve incluir controles como cópias de segurança, uso de senhas, controle de acesso, atualização de softwares, e uso de antivírus, conforme orientação da ANPD.
- Crie um Plano de Resposta a Incidentes com etapas de identificação, contenção, remoção de ameaças, recuperação de sistemas e comunicação.
- Defina cronogramas para revisar e atualizar documentos de proteção de dados, como a Política de Privacidade, Termos de Uso e o Relatório de Impacto à Proteção de Dados (RIPD).
- Estabeleça políticas de descarte de informações pessoais, com orientações para registro e destruição de mídias e arquivos físicos.
- Adote contratos com cláusulas robustas de confidencialidade e proteção de dados pessoais, incluindo um patamar mínimo de medidas esperado pela empresa e a assinatura de acordos de confidencialidade e proteção de dados com quem irá acessar dados pessoais dentro do ente de saúde.

As pessoas de uma instituição são um pilar essencial para a segurança da informação pois são as responsáveis por entender e aplicar efetivamente os procedimentos de segurança, pondo em prática a cultura organizacional que preze pela política adotada. Nesse sentido, os funcionários e colaboradores compõem um grupo que merece atenção das instituições, que deve estar engajado e ser capacitado com as melhores práticas, já que este grupo pode identificar no cotidiano da instituição atividades suspeitas à segurança da informação e responderem apropriadamente.

Para funcionários e colaboradores, o princípio do menor privilégio (ou "need to know") orienta que os indivíduos ou sistemas devem ter acesso apenas às informações ou recursos que são necessários para o desempenho de suas funções específicas. Assim, esse princípio minimiza a exposição de dados sensíveis e reduz o alcance de possíveis incidentes,

limitando o impacto de uma possível violação de segurança e pode ser adotado pelas instituições em sua estratégia de segurança da informação.

Programas de treinamento e conscientização para as pessoas de uma organização são relevantes e podem incluir medidas como:

RECOMENDAÇÕES PARA CONSCIENTIZAÇÃO DAS PESSOAS **SOBRE SEGURANÇA DA INFORMAÇÃO**

- Treinamentos sobre as obrigações legais e responsabilidades dispostas pela LGPD e atualizações emitidas pela ANPD a respeito do tratamento de dados pessoais devem compor o calendário da instituição, em especial para quem atua diretamente com o tratamento de dados pessoais.
- Explique o uso de controles de segurança nos sistemas de Tecnologia da Informação no cotidiano do trabalho.
- Oriente sobre o uso seguro de logins e senhas, o que inclui o uso de senhas fortes, exclusivas, e que não sejam compartilhadas com terceiros, por exemplo, bem como não utilizar senhas padrão disponibilizadas pelos fornecedores de sites e aplicativos. As empresas podem desenvolver neste sentido políticas de uso e atualização de senhas, com recomendações a serem seguidas pelos funcionários.
- Treine seus funcionários e colaboradores para identificação de e-mails fraudulentos e ações que as impeçam de serem vítimas de fraudes comuns, como cliques em links desconhecidos que podem ocasionar ataques de phishing.
- Desenvolva medidas conhecidas como "mesa limpa", ou seja, para evitar que documentos físicos que contenham dados pessoais estejam expostos ou acessíveis facilmente sobre as mesas, por exemplo.
- Considere a realidade da sua equipe para oferecer treinamentos personalizados. No ambiente profissional, por exemplo, apresente orientações quanto à conduta dos funcionários no uso de equipamentos para que, ao se deslocarem da estação de trabalho, optarem pelo bloqueio de telas e dispositivos utilizados, como computadores. No caso de trabalhadores remotos, se possível, forneça equipamentos funcionais e oriente sobre as boas práticas que devem ser adotadas no seu uso.
- Capacite de forma específica, conforme a realidade de cada setor da empresa, as pessoas para manuseio e descarte adequado de documentos que contenham dados pessoais, em especial, dados pessoais sensíveis.
- Revise documentos internos como o manual ou o código de conduta de seus funcionários para incluir a importância da privacidade e segurança da informação.
- Explique e compartilhe os documentos e atualizações sobre proteção de dados e segurança da informação da sua instituição, incluindo treinamentos para as hipóteses de identificação de incidentes de segurança.
- Conscientize a respeito do cuidado no compartilhamento dos dados, especialmente de saúde, seja via e-mail, aplicativos de comunicação (whatsapp), outros, ou até mesmo por telefone; a fim de garantir que as informações sejam entregues de forma segura, minimamente o necessário e às pessoas certas.

Pode-se fornecer orientações contra as principais técnicas de ameaça à segurança da informação, tanto para seus funcionários, como clientes e parceiros comerciais. Providencie canais oficiais e seguros para atendimento, que utilizem preferencialmente domínios próprios em e-mails, e forneça materiais informativos que se adequem à realidade de sua instituição com recomendações de boas práticas.

ORIENTAÇÕES CONTRA OS **PRINCIPAIS RISCOS À SEGURANÇA CIBERNÉTICA**

- Desconfie de mensagens não solicitadas: se receber um e-mail, mensagem de texto ou ligação de um remetente desconhecido, seja cauteloso.
- Verifique a autenticidade do remetente: antes de clicar em qualquer link ou abrir anexos, verifique se o endereço de e-mail ou o número de telefone são legítimos.
- Não forneça informações pessoais por e-mail ou telefone: jamais forneça senhas, números de cartão de crédito ou outras informações confidenciais por e-mail, mensagem de texto ou telefone, a menos que você tenha iniciado o contato.
- Utilize senhas fortes e únicas: crie senhas complexas e exclusivas para cada conta e utilize um gerenciador de senhas.
- Mantenha seus softwares atualizados: instale as atualizações de segurança para seus sistemas operacionais, aplicativos e softwares.

- Utilize um bom programa de antivírus: contribui para a proteção de seu dispositivo contra malwares e acessos indevidos.
- Contrate serviços de mitigação de DDoS em sua organização que sejam especializados, para que possam detectar e mitigar ataques DDoS, garantindo a continuidade do serviço.
- Esteja atento aos sinais de phishing e demais modalidades de fraudes: se atente em erros de ortografia, links suspeitos, solicitações de informações pessoais e um senso de urgência.

Além disso, deve-se considerar os parceiros contratuais, com quem há compartilhamento de dados e informações sensíveis. Para os parceiros, medidas como análise prévia para verificar se atendem às condições de cumprimento à LGPD e segurança são importantes.

BOAS PRÁTICAS CONTRATUAIS PARA A SEGURANÇA DA INFORMAÇÃO

- Inicialmente, é importante que as instituições invistam na adequação à LGPD, com o mapeamento de dados e o fluxo de informações em seus sistemas e procedimentos utilizados.
- Realize investigações prévias às contratações e avalie se seus parceiros com quem há compartilhamento de dados pessoais cumpre com as condições mínimas de segurança da informação, a depender da complexidade.
- Os contratos podem ser elaborados ou revisado com cláusulas que garantam a segurança da informação, em especial, para os serviços em nuvem.
- Em contratos de serviço, quando aplicável, estabeleça cláusulas com indicação do registro da destruição ou descarte das informações.
- Revise os contratos de sua organização para estabelecer as cláusulas de segurança da informação que assegurem a proteção de dados pessoais como, por exemplo, determinações sobre compartilhamento de dados e orientações quanto à relação controlador-operador.
- Firme termos de confidencialidade (NDA - non-disclosure agreement) com os funcionários da organização.
- Estabeleça contratos de Processamento de Dados (DPA - data processing agreement) quando houver o compartilhamento de dados, com especificações sobre as garantias no âmbito da segurança da informação.

No campo das medidas tecnológicas, os equipamentos e sistemas utilizados devem permitir que as informações devem estar resguardadas de ataques de hackers, negligência ou acesso não autorizado e, para além das medidas administrativas e treinamento humano, os equipamentos e tecnologias utilizadas pelas instituições devem atender a bons padrões de qualidade e segurança.

BOAS PRÁTICAS DE SEGURANÇA DA **INFORMAÇÃO NO USO DE FERRAMENTAS TECNOLÓGICAS**

- Realize o monitoramento contínuo de atividades suspeitas, com análise periódica de sistemas e dispositivos utilizados pela instituição.
- Adote e atualize de forma regular softwares de proteção das informações, como antivírus e antimalwares.
- No caso de e-mails, adote ferramentas que criem filtros de e-mail, com AntiSpam, e que estejam integradas aos programas de antivírus e antimalwares.
- Implemente medidas para pseudonimização, como a criptografia de dados pessoais. Dados de pacientes devem ser armazenados preferencialmente em pastas de nuvem criptografadas ou, quando em arquivos físicos, em locais de acesso controlado e com registro de acesso.
- Instale sistemas de firewall e/ou opte por utilizar um Web Application Firewall (WAF – Filtro de Aplicação), para monitorar e controlar o tráfego de entrada e saída, bloqueando acessos não autorizados.
- Desenvolva procedimentos de registros que sejam confiáveis, que envolvam, por exemplo, a manutenção do histórico de solicitações para acesso a certos dados. Para acesso às informações relevantes, como os dados de saúde de pacientes, mantenha o registro de quem, quando, e por qual motivo há o acesso a tais dados.
- Evite o uso de sistemas obsoletos e regularmente atualize os atualize através das atualizações emitidas pelos próprios fornecedores contra vulnerabilidades de segurança e para otimização do desempenho de dispositivos e softwares.
- Adote a autenticação multifator em seus dispositivos, inclusive para permitir o controle de dispositivos móveis (como celulares e laptops), exigindo mais do que apenas uma senha para autenticação.
- Implemente medidas de segurança de acesso controlado, que podem incluir o bloqueio de impressoras e a restrição de acesso a funcionalidades, dependendo de quem está utilizando o sistema.
- Quando do uso de equipamentos funcionais, não utilize redes de Wi-Fi públicas e, se possível, faça a distinção de uso de dispositivos privados em relação aos de uso funcional.
- Adote técnicas para a segurança das comunicações, como por meio do uso de conexões cifradas (TLS/HTTPS) ou demais aplicativos com criptografia fim-a-fim.
- Se possível, opte por utilizar redes privadas virtuais (VPN), como forma de proteger as conexões de rede.
- Adote normas técnicas e certificações reconhecidas para garantia da segurança da informação, como, por exemplo, as emitidas da Associação Brasileira de Normas Técnicas (ABNT) ou da International Organization for Standardization (ISO).
- No caso de dispositivos móveis, opte por funcionalidades que possibilitem remotamente a exclusão de dados pessoais armazenados.

Vale destacar que a segurança da informação de saúde pessoal é elencada como um dos direitos dos indivíduos na Portaria GM/MS nº 1.768/2021, que define a Política Nacional de Informática e Informações em Saúde (PNIIS), bem como orienta as instituições quanto ao engajamento do usuário como protagonista da sua saúde e para promoção de um ecossistema de inovação no setor de saúde. No campo da informatização das instituições de saúde, privadas e públicas, constam dentre as diretrizes da PNIIS o fortalecimento do "uso de mecanismos de segurança de acesso aos sistemas, dados e informações de saúde", como forma de resguardar a "disponibilidade, autenticidade e integridade" das informações (Art. 5º, V):

DIRETRIZES DA PNIIS PARA INFORMATIZAÇÃO DAS INSTITUIÇÕES

- Indução à informatização com padrão mínimo para infraestrutura e segurança de TIC (tecnologia da informação e comunicação) a ser alcançado, de forma a acelerar a adoção de sistemas de prontuários eletrônicos, de apoio à decisão e de gestão como parte integradora dos serviços e processos de saúde (Art. 5º, I).
- Estímulo ao uso de sistemas de prontuário eletrônico com segurança e funcionalidades compatíveis com os processos de trabalho em saúde e adequadas para atender à realidade das diferentes esferas de gestão e níveis de complexidade da saúde, bem como dos estabelecimentos de saúde considerando as necessidades dos setores público e privado, para atendimento aos padrões de intercâmbio de dados com a RNDS (Rede Nacional de Dados em Saúde) (Art. 5º, II).
- Promoção da articulação com o Ministério da Ciência, Tecnologia, Inovações, com o Ministério das Comunicações, e com agências reguladoras federais, com vistas à implantação da infraestrutura e procedimentos necessários à área de saúde digital (Art. 5º, III).
- Fornecimento de TIC adequada para o recebimento do histórico clínico pela RNDS ao longo de todo ciclo de vida do usuário, para continuidade de cuidado, por meio de prontuário eletrônico das instituições públicas e privadas, em conformidade com as diretrizes legais sobre gestão documental, dispostas na Lei nº 8.159, de 8 de janeiro de 1991, e no Decreto nº 4073 de 3 de janeiro de 2002 (Art. 5, IV).
- Promoção do uso de mecanismos de segurança de acesso aos sistemas, dados e informações de saúde, que garantam sua disponibilidade, autenticidade e integridade, com incentivo ao uso de assinatura eletrônica e sistemas biométricos (Art. 5º, V).
- Promover a padronização dos modelos de informação mínimos nacionais, bem como dos vocabulários e terminologias em saúde (Art. 5º, VI).

Por fim, vale considerar que ataques à segurança da informação colocam em risco a proteção de dados dos titulares, a integridade dos serviços prestados e podem representar sérios riscos financeiros e institucionais para as organizações. As transformações tecnológicas exigem acompanhamento periódico das organizações, para que possam se manter atualizadas e aprimorar suas ações, com rapidez e eficiência em suas ações.

12. INOVAÇÃO NO SETOR DE SAÚDE

O avanço tecnológico no setor da saúde tem proporcionado soluções inovadoras para o diagnóstico, tratamento e acompanhamento de doenças. Além disso, o desenvolvimento de pesquisas no campo da saúde através do uso de tecnologias como a inteligência artificial, realidade aumentada e virtual, e internet das coisas é crucial para permitir o aprimoramento de técnicas e avanços que aprimoram desde a gestão de sistemas de saúde, para melhoria da qualidade do atendimento, personalização de tratamentos, otimização de processos internos e impactam no cuidado direto com os pacientes.

EXEMPLOS DE INOVAÇÕES PARA PROMOÇÃO DA SAÚDE DE PACIENTES **POR PRESTADORES DE SERVIÇOS DE SAÚDE**

- Uso de dispositivos de saúde e vestíveis conectados nas residências que podem permitir consultas médicas remotas (telessaúde).
- Manutenção preventiva de equipamentos hospitalares a partir de suas condições, reduzindo custos e promover a oferta de serviços com mais qualidade.
- Desenvolvimento e treinamento de mecanismos de Inteligência Artificial na Saúde.

EXEMPLOS DE INOVAÇÕES PARA PROMOÇÃO DA SAÚDE DE PACIENTES **POR OPERADORAS DE PLANOS DE SAÚDE**

- Os pacientes podem fazer uso de dispositivos para monitoramento de sua saúde, permitindo que eles tenham gerenciamento praticamente em tempo real e, com a orientação dos profissionais de saúde, atuarem com mais informação para a sua própria qualidade de vida e segurança.
- Alocação eficiente de recursos médicos, identificação de fraudes e redução de custos operacionais.

EXEMPLOS DE INOVAÇÕES PARA PROMOÇÃO DA SAÚDE DE PACIENTES **POR FORNECEDORES E DISTRIBUIDORES DE PRODUTOS PARA SAÚDE**

- Os procedimentos de saúde, como cirurgias, podem ser realizados com tecnologias que podem ser ingeridas ou injetadas, reduzindo o grau de risco e de custos de procedimentos padrões.
- O rastreamento de medicações e dispositivos médicos pode reduzir falsificações.

No entanto, a crescente coleta, tratamento e o uso de dados sensíveis dos pacientes exigem uma atenção especial à proteção de dados. O incentivo à inovação no setor de saúde deve estar acompanhado da atenção aos direitos fundamentais, sendo recomendável a elaboração de Relatório de Impacto à Proteção de Dados Pessoais.

Dessa forma, destacaremos outras boas práticas e medidas de mitigação de risco que podem ser adotadas para i) desenvolvimento de novas tecnologias; ii) realização de pesquisas em saúde; iii) uso de biometria; iv) utilização de IA em saúde.

12.1. DESENVOLVIMENTO DE NOVAS TECNOLOGIAS E "PRIVACY BY DESIGN"

A LGPD, em seus artigos 46 e 50, orienta os agentes de tratamento a adotarem medidas de segurança e mitigação de riscos que abrangem todo o ciclo de vida dos dados, tanto em meios físicos quanto digitais. Essas medidas são essenciais para garantir a proteção adequada dos dados pessoais em todas as fases de seu tratamento e corroboram para a criação de uma cultura de proteção de dados.

Nesse contexto, é fundamental que as equipes responsáveis pelo desenvolvimento de serviços e produtos incorporem a privacidade desde a concepção de suas ações, promovendo a efetividade de um programa de privacidade. Essa abordagem proativa, conhecida como Privacy by Design, deve ser implementada pelas organizações e está pautada nos seguintes princípios:

PRINCÍPIOS DA PRIVACIDADE **NA CONCEPÇÃO, OU PRIVACY BY DESIGN**

- Proatividade, e não reatividade.
- Prevenção, e não reparação.
- Privacidade como padrão.
- Privacidade incorporada ao design.
- Total funcionalidade – resultado positivo, e não soma zero.
- Segurança do começo ao final – proteção do ciclo de vida.
- Visibilidade e transparência.
- Respeito pela privacidade do usuário.

EDPS. Opinion 5/2018 - Preliminary Opinion on privacy by design. 2018. Disponível em: https://www.edps.europa.eu/sites/default/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

Tradução livre de: C AVOUKIAN, Ann. Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices. 2017. Disponível em: http://dataprotection.industries/wp-content/uploads/2017/10/privacy-by-design.pdf.

A abordagem de Privacy by Design busca garantir a proteção dos dados pessoais desde a concepção até a implementação de novas tecnologias, em conformidade com as legislações vigentes. Na prática, a aplicação deste conceito no setor da saúde significa que os desenvolvedores de tecnologias devem considerar a privacidade como um elemento central. Isso inclui a adoção de medidas técnicas, como criptografia e anonimização dos dados, e organizacionais, como a limitação de acesso a informações sensíveis apenas a profissionais autorizados.

EXEMPLOS DO **USO DO PRIVACY BY DESIGN** NO SETOR DE SAÚDE

- Os prestadores de serviços de saúde podem implementar medidas de pseudonimização em registros eletrônicos de saúde (EHR) para que a identidade dos pacientes seja substituída por códigos, dificultando a identificação direta, e revelada apenas quando necessário. Além disso, podem estabelecer controle de acesso com base nas funções desempenhadas por cada funcionário, para que apenas os funcionários de saúde tenham acesso aos dados pessoais sensíveis de pacientes na prestação do serviço de saúde.
- As operadoras de planos de saúde podem estabelecer a criptografia de ponta a ponta em suas comunicações, para que o envio de dados para autorização de procedimentos seja seguro. Outra medida que pode ser utilizada se refere às ações para a coleta do consentimento informado por granularidade, em que são fornecidos mecanismos para que o titular, de forma específica e segmentada, avalie e decida a respeito da sua concessão do consentimento conforme cada tratamento.
- Os fornecedores e distribuidores de produtos para saúde podem incorporar a proteção de dados desde a concepção de produtos, garantindo que apenas informações essenciais sejam coletadas e que os dados sejam processados de forma segura, acessados apenas pelos profissionais habilitados e com criptografia integrada. Ademais, podem utilizar tecnologias blockchain para garantir que os sistemas com informações sobre a rastreabilidade de produtos estejam protegidos.

Nesse sentido, o desenvolvimento de novas tecnologias no setor de saúde pode considerar elementos como:

RECOMENDAÇÕES PARA A INOVAÇÃO NO SETOR DE SAÚDE COM A **ABORDAGEM DO PRIVACY BY DESIGN**

- Envolva profissionais de privacidade no processo de design e desenvolvimento dos serviços e produtos.
- Processe dados de acordo com a estrita necessidade e finalidade informada ao titular.
- Ao processar um dado pessoal, tenha certeza de que os todos os agentes, fornecedores, sistemas e serviços utilizados no tratamento de dados – em todas as etapas do tratamento – adotem medidas técnicas e operacionais para proteção dos dados.
- Implemente tecnologias e práticas que melhorem a privacidade, como criptografia e minimização de dados.
- Previna riscos de incidentes de segurança como regra para que eles não ocorram ou, caso ocorram, para que medidas sejam adotadas o mais rápido possível.

- Garanta que os titulares não precisem tomar nenhuma ação específica para proteger seus dados pessoais quando da utilização dos seus sistemas. Assim, ao adotar a privacidade como padrão, os indivíduos não devem ter o ônus de se esforçar para obter proteção ao usar um serviço ou produto, já que a proteção é garantida "automaticamente".
- Apresente informações sobre os encarregados pelo tratamento de dados.
- Utilize linguagem acessível em documentos públicos para facilitar a compreensão dos usuários e possibilitar que os usuários possam gerenciar a forma como seus dados são tratados.
- Utilize tecnologias de aprimoramento de privacidade (PETs) para auxiliar no cumprimento de suas obrigações.
- Periodicamente revise e atualize as políticas e procedimentos de privacidade da usa organização para garantir a conformidade com as leis e regulamentos vigentes.

Recomendações elaboradas a partir de: ICO. Data protection by design and default. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-andgovernance/data-protection-by-design-and-default/; PRIVACYENGINE. Understanding Privacy by Design Principle. Disponível em: https://www.privacyengine.io/blog/understanding-privacy-by-design-principles/.

A ANPD, em seu Guia Orientativo sobre cookies e proteção de dados pessoais, apresentou recomendações e exemplos visuais com boas práticas de privacy by design. Dentre as orientações expostas pela Autoridade, é possível destacar o fomento para o uso de mecanismos diretos que exponham de forma organizada as informações aos titulares e possibilite de forma facilitada a escolha dos titulares, como a personalização das escolhas para gerenciamento do consentimento e destaques visuais aos botões de aceite. Essas medidas colaboram não apenas com a compreensão e visualização do conteúdo, mas também com a tomada de decisão qualificada por parte dos titulares, em atenção ao determinado pela LGPD.

Ao adotar técnicas de Privacy by Design, as organizações não apenas cumprem com as leis de proteção de dados, mas também fortalecem sua reputação, aumentam a confiança dos clientes e se diferenciam no mercado. Essa abordagem proativa permite que as empresas estejam preparadas para seguir com o desenvolvimento de tecnologias, enfrentando os desafios de privacidade em um mundo digital em constante evolução.

12.2 REALIZAÇÃO DE PESQUISAS EM SAÚDE

O tratamento de dados pessoais para a execução de pesquisas é necessário pois auxilia na garantia do direito à saúde, promovendo a inovação e avanços que podem beneficiar a sociedade como um todo.

EXEMPLOS DE **PESQUISAS EM SAÚDE**

- Os prestadores de serviços de saúde podem utilizar as informações de saúde para descobrir novas causas e tratamentos para doenças; avaliar a eficácia de diferentes intervenções em saúde.
- As operadoras de planos de saúde podem aprimorar as técnicas de gestão de sistemas de saúde, com identificação das necessidades de certo grupo de pessoas e alocação mais eficiente de recursos.
- Os fornecedores e distribuidores de produtos para saúde podem aprimorar a produção e funcionalidade de equipamentos e dispositivos utilizados para promoção da saúde, com técnicas que sejam menos invasivas aos pacientes.

Assim, o desenvolvimento de pesquisas em saúde exige constante tecnologia e inovação, sendo relevante para o desenvolvimento industrial do país, já que orienta a produção de medicamentos, imunobiológicos, vacinas, equipamentos e dispositivos médicos para diagnóstico e cuidado da saúde, bem como demais derivados. As pesquisas também contribuem para o fornecimento de evidências científicas que auxiliam a tomada de decisões em saúde com mais solidez.

No caso do tratamento de dados pessoais, é necessário avaliar cuidadosamente as condições para a legitimidade desta atividade. Para tanto, destacam-se os princípios da necessidade, finalidade, adequação e transparência. Com relação a este último, os titulares devem ser informados individualmente sobre a "existência da operação de tratamento e o fato de que seus dados pessoais (de saúde) estão sendo tratados para fins científicos".

Outro ponto de atenção se refere ao uso secundário de dados pessoais. A LGPD não proíbe o uso secundário de dados pessoais, desde que o novo tratamento seja compatível com as finalidades que justificarem o tratamento original: com o objetivo de "investigação científica, histórica ou estatística". De acordo com a ANPD, há nestas hipóteses uma "presunção de compatibilidade" para as finalidades mencionadas, com destaque aos tratamentos realizados por órgãos de pesquisa.

Acontece que a definição "órgãos de pesquisa" não abarca as entidades com fins lucrativos, apenas pessoas jurídicas sem finalidade de lucro (art. 5º, XVIII). Isso quer dizer que diversas entidades do ramo da saúde não estão habilitadas a utilizar essa justificativa para suportar suas atividades de pesquisa. Nesse caso, a depender de como o estudo será conduzido, é importante focar na utilização de mecanismos de transparência e de segurança, na adoção de outra hipótese legal adequada e, especialmente, em técnicas de anonimização e pseudonimização, para garantir a utilização segura dos dados.

GUIMARÃES, Reinaldo. Pesquisa em saúde no Brasil: contexto e desafios. Revista de Saúde Pública, v. 40, p. 3-10, 2006.

EDPB. Diretrizes 03/2020 sobre o tratamento de dados relativos à saúde para efeitos de investigação científica no contexto do surto de COVID-19. 2020, p. 8. Disponível em: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_pt.pdf.

CNS. Código de boas práticas – proteção de dados para prestadores privados em saúde. 2021, p. 118. Para a realização de pesquisa clínica, por exemplo, é possível que os dados sejam coletados a partir das informações de saúde do paciente (como o resultado de seus exames), ou através do cruzamento de dados.

ANPD. Guia Orientativo – Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas. Jun/2023, p. 11. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf.

ANÁLISE PRÉVIA PARA PERMITIR **O TRATAMENTO SECUNDÁRIO DE DADOS PESSOAIS**

- A ANPD recomenda que os responsáveis pelo tratamento de dados considerem os seguintes pontos:
- a natureza dos dados pessoais, adotando-se maior cautela quando abrangidos dados sensíveis;
- as expectativas legítimas dos titulares e os possíveis impactos do tratamento posterior sobre seus direitos;
- os princípios da LGPD, em especial os da finalidade, adequação, necessidade, transparência e não discriminação;
- as medidas de prevenção e segurança apropriadas; e os padrões éticos aplicáveis à hipótese.

Tais recomendações devem ser observadas inclusive quando os dados são tornados manifestamente públicos pelo titular. Nesta hipótese, deve-se respeitar "os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos" na LGPD (Art. 7º, § 7º).

No âmbito da pesquisa em saúde, o princípio da finalidade tem sido tensionado pelo avanço da tecnologia, já que a metodologia tradicional, em que há uma hipótese bem delimitada, tem sido substituída por outra, na qual não há a definição dos dados pertinentes para a pesquisa, mas um grande volume de dados é utilizado como insumo para se identificar padrões. Com base nessa metodologia, não é possível definir-se um propósito específico que justifique o tratamento de dados, já que os dados necessários para a condução da pesquisa são identificados depois de tratados.

Diante dos desafios impostos pelas novas tecnologias na área de saúde, De acordo com Andréa Gobbato, "embora a LGPD não faça menção explícita, a identificação de uma nova base legal para o tratamento posterior não parece ser necessária caso o tratamento seja compatível. A noção de compatibilidade não apenas permite que os dados rejam reaproveitados, sem necessidade de nova coleta, mas também que o tratamento posterior compatível seja considerado coberto pela base legal que justificou o propósito primário da coleta dos dados".

Ou seja, o tratamento secundário de dados é possível quando a finalidade secundária for compatível com a finalidade que justificou o tratamento no primeiro momento, sem que seja necessária uma nova base legal. Insta ressaltar que caso o consentimento seja utilizado como base legal, é necessário que ele seja obtido de maneira livre e informado plenamente, com indicações inequívocas, específicas e destacadas para a finalidade da pesquisa. Ainda, é necessária a "obtenção do consentimento dos participantes de pesquisa, quando assim exigido pelas normas e padrões éticos aplicáveis", de acordo com orientações da ANPD.

ANPD. Guia Orientativo – Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas. Jun/2023, p. 11. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf.

ANPD. Guia Orientativo – Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas. Jun/2023, p. 12. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf. Grifos originais.

GOBBATO, Andréa Guimarães. Princípio da finalidade e tratamento de dados de saúde: análise contextual de proteção de dados, saúde e inovação. 2025. Universidade de São Paulo, Dissertação de Mestrado. P. 203

GOBBATO, Andréa Guimarães. Princípio da finalidade e tratamento de dados de saúde: análise contextual de proteção de dados, saúde e inovação. 2025. Universidade de São Paulo, Dissertação de Mestrado. P. 157.

ANPD. Guia Orientativo – Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas. Jun/2023, p. 56. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf.

A Lei Federal nº 14.784/2024, e a Resolução nº 510, de 7 de abril de 2016, do Conselho Nacional de Saúde, vinculado ao Ministério da Saúde, apresentam os seguintes conceitos pertinentes ao assunto:

CONCEITOS RELEVANTES PARA **A ELABORAÇÃO DE PESQUISAS NA SAÚDE**

LEI Nº 14.784/2024

Consentimento livre e esclarecido: "anuência do participante da pesquisa ou de seu representante legal, livre de simulação, fraude, erro ou intimidação, após esclarecimento sobre a natureza da pesquisa, sua justificativa, seus objetivos, métodos, potenciais benefícios e riscos" (Art. 2º, V).

Assentimento: "anuência da criança, do adolescente ou do indivíduo legalmente incapaz em participar voluntariamente da pesquisa, após ter sido informado e esclarecido sobre todos os aspectos relevantes de sua participação, na medida de sua capacidade de compreensão e de acordo com suas singularidades, sem prejuízo do necessário consentimento dos responsáveis legais" (Art. 2º, II).

Termo de Consentimento Livre e Esclarecido (TCLE): "documento no qual é explicitado o consentimento livre e esclarecido do participante da pesquisa, ou do seu responsável legal, de forma escrita, com todas as informações necessárias, em linguagem clara e objetiva, de fácil entendimento, para o completo esclarecimento sobre a pesquisa da qual se propõe participar" (Art. 2º, LIII).

Esclarecimento: "processo de apresentação clara e acessível da natureza da pesquisa, sua justificativa, seus objetivos, métodos, potenciais benefícios e riscos, concebido na medida da compreensão do participante, a partir de suas características individuais, sociais, econômicas e culturais, e em razão das abordagens metodológicas aplicadas. Todos esses elementos determinam se o esclarecimento dar-se-á por documento escrito, por imagem ou de forma oral, registrada ou sem registro" (Art. 2º, X).

RESOLUÇÃO CNS Nº 510/2016

Consentimento livre e esclarecido: "manifestação do indivíduo, ou de seu representante legal, mediante assinatura de termo de consentimento livre e esclarecido, de sua disposição de participar voluntariamente da pesquisa, após ter sido informado e esclarecido sobre todos os aspectos relevantes para a tomada de decisão sobre sua participação" (Art. 2º, XIII)

Assentimento livre e esclarecido: "anuência do participante da pesquisa – criança, adolescente ou indivíduos impedidos de forma temporária ou não de consentir, na medida de sua compreensão e respeitadas suas singularidades, após esclarecimento sobre a natureza da pesquisa, justificativa, objetivos, métodos, potenciais benefícios e riscos. A obtenção do assentimento não elimina a necessidade do consentimento do responsável" (Art. 2º, I).

Registro do consentimento ou do assentimento: "documento em qualquer meio, formato ou mídia, como papel, áudio, filmagem, mídia eletrônica e digital, que registra a concessão de consentimento ou de assentimento livre e esclarecido, sendo a forma de registro escolhida a partir das características individuais, sociais, linguísticas, econômicas e culturais do participante da pesquisa e em razão das abordagens metodológicas aplicadas" (Art. 2º, XIII).

O registro do assentimento e do consentimento deve ser realizado antes do início de qualquer procedimento de estudo. No caso do Termo para o consentimento, a Lei nº 14.874/2024 exige que seja escrito, em "linguagem de fácil compreensão e somente terá validade quando for datado" e assinado pelo pesquisador responsável e pelo participante da pesquisa ou por seu representante legal ou, se o participante da pesquisa ou seu representante legal não seja capaz de ler, por testemunha imparcial (Art. 18, §§ 1º e 5º, da Lei nº 14.874/2024).

O registro do consentimento pode ser obtido por documento de qualquer meio, formato ou mídia que registre a concessão do titular. A forma de registro da escolha do titular deve ser selecionada "a partir das características individuais, sociais, linguísticas, econômicas e culturais do participante da pesquisa e em razão das abordagens metodológicas aplicadas" (Art. 2º, XXII, da Resolução CNS nº 510/2016).

ORIENTAÇÕES PARA ELABORAÇÃO DO **TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO EM ATENÇÃO À PROTEÇÃO DE DADOS PESSOAIS**

- Apresente a identificação dos responsáveis e instituições envolvidas. Sua organização pode adotar modelos de cabeçalho e pré-texto de identificação.
- Apresente de forma clara e objetiva o teor da pesquisa, "os objetivos e os procedimentos que serão utilizados na pesquisa, com informação sobre métodos a serem utilizados, em linguagem clara e acessível, aos participantes da pesquisa, respeitada a natureza da pesquisa" (Art. 17, I, da Resolução CNS nº 510/2016).
- Indique as informações sobre o(s) responsável(eis) pela pesquisa, com os quais o titular possa entrar em contato. A Resolução CNS nº 510/2016 exige o endereço, e-mail e contato telefônico (Art. 17, VIII). É possível ainda a indicação do horário de funcionamento da organização, do site da instituição, pois estas informações auxiliam os titulares no exercício de seus direitos.
- No momento da assinatura, indique que o titular pode "fornecer ou não seu consentimento para possíveis usos futuros em pesquisa de seus dados e material biológico" (Art. 40, X, da Lei nº 14.784/2024).
- Informe que o titular pode decidir por não continuar participando do estudo em qualquer momento e que esta decisão não gera qualquer ônus, punição ou perda de benefícios das quais o titular tenha direito (Art. 17, III, da Resolução CNS nº 510/2016). Além disso, o titular tem direito à devolução das amostras quando do uso de material biológico humano (Art. 40, IV, da Lei nº 14.784/2024).
- Forneça a cópia do documento que comprove a assinatura/concessão do consentimento do titular. Além disso, informe que o titular poderá a qualquer momento ter acesso ao registro do consentimento (Art. 17, X, da Resolução CNS nº 510/2016).
- Indique que são garantidas a manutenção do sigilo e da privacidade em todas as etapas da pesquisa, com exceção da manifestação explícita do próprio titular em sentido contrário (Art. 17, IV, da Resolução CNS nº 510/2016).
- Explique sobre os possíveis benefícios e riscos da participação do titular no estudo, além de garantir que os profissionais (médico-investigador) estejam disponíveis para demais explicações junto aos titulares (Art. 17, II, da Resolução CNS nº 510/2016).
- Apresente brevemente explicações sobre o que é o Comitê de Ética em Pesquisa (CEP), bem como endereço, e-mail e contato telefônico do CEP local e, quando for o caso, da Comissão Nacional de Ética em Pesquisa (CONEP) (Art. 17, IX, da Resolução CNS nº 510/2016).
- Por determinação da Lei nº 14.784/2024, os direitos dos participantes da pesquisa devem constar obrigatoriamente no TCLE (Art. 40, § único). A Lei elenca as seguintes previsões:
- Ser devidamente informado e esclarecido, de forma clara e objetiva, sempre que julgar pertinente, sobre o objeto e os potenciais benefícios e riscos inerentes à disposição de seu material biológico (Art. 40, I).
- Ter a sua saúde e a sua integridade, física e mental, protegidas durante os procedimentos de coleta do material biológico (Art. 40, II).
- Retirar a qualquer tempo o consentimento de guarda e de utilização do material biológico humano armazenado, por escrito e assinado, sem ônus ou prejuízos, tendo direito à devolução das amostras (Art. 40, III).
- Ter acesso, a qualquer tempo, sem ônus ou prejuízo, às informações sobre as finalidades do armazenamento, incluídos os nomes dos responsáveis técnicos e institucionais, os riscos e os benefícios potenciais, as garantias de qualidade da conservação e a integridade do seu material biológico (Art. 40, IV).
- Ter acesso, a qualquer tempo, sem ônus ou prejuízo, às informações associadas a seu material biológico e ser informado e orientado pelos pesquisadores responsáveis por achados quando as implicações dessas informações puderem causar danos à sua saúde, incluído o aconselhamento genético quando cabível (Art. 40, V).
- Ter garantidas a privacidade e a confidencialidade de suas informações pessoais (Art. 40, VI).
- Ser prontamente informado sobre a dissolução do repositório no qual se encontra armazenado o seu material biológico (Art. 40, VII).
- Ser prontamente informado sobre a transferência, a perda, a alteração ou o descarte do seu material biológico (Art. 40, VIII).

- Designar representantes legais que poderão consentir com a utilização e o descarte do seu material biológico e ter acesso a esses materiais e a suas informações associadas em caso de óbito ou de condição incapacitante (Art. 40, IX).
- Ser esclarecido, no momento da assinatura do TCLE, sobre a possibilidade de fornecer ou não seu consentimento para possíveis usos futuros em pesquisa de seus dados e material biológico (Art. 40, X).
- Ser esclarecido, no momento da assinatura do TCLE, sobre a possibilidade de autorizar ou não o envio de seus dados e material biológico para centro de pesquisa localizado fora do País (Art. 40, XI).

Ressalte-se que quando o tratamento de dados pessoais se fundamenta na base legal do consentimento, a LGPD não exige a obtenção de um novo consentimento para usos secundários. A legislação determina que o titular seja informado sobre eventual alteração da finalidade originalmente consentida apenas quando essa nova finalidade for incompatível com o consentimento previamente fornecido, assegurando-lhe, nesse caso, o direito de revogá-lo a qualquer tempo (Art. 9º, §2º).

Em relação à aplicação da base legal para realização de estudos por órgão de pesquisa, no caso de órgãos que realizam estudos em saúde pública, a LGPD estabelece em seu Art. 13 como obrigações:

o tratamento de dados pessoais deve ocorrer exclusivamente dentro do órgão;

o tratamento deve ser estrito à finalidade de realização de estudo e pesquisa;

manutenção dos dados em ambiente controlado e sveguro;

sempre que possível, os dados devem ser anonimizados ou pseudonimizados;

devem ser observados os padrões éticos relativos aos estudos e pesquisas, como nos casos de Códigos de Ética em Pesquisa da instituição.

No caso de disponibilização de acesso a dados pessoais, deve-se avaliar a natureza do agente de tratamento que receberá as informações. Conforme recomendado pela ANPD, na hipótese de ser um órgão de pesquisa que recebe o material para estudos, é possível o uso da base legal para realização de estudos por órgão de pesquisa (Art. 7º, IV, ou Art. 11, II, c, da LGPD). Caso o órgão seja de outra natureza, devem ser consideradas as outras bases legais, como o consentimento ou o legítimo interesse.

Além da avaliação das condições de legitimidade para o tratamento de dados, as pesquisas podem adotar as seguintes boas práticas para a proteção de dados pessoais:

SALVAGUARDAS PARA O USO DE DADOS PESSOAIS EM PESQUISAS

- Analise com cautela as bases legais e princípios aplicáveis para garantir a legalidade do tratamento e o respeito fundamental do direito à proteção de dados pessoais. Nesta etapa, é recomendável a documentação, para registro da justificativa das escolhas adotadas pelos agentes de tratamento.
- Opte pela minimização de dados pessoais, utilizando o estritamente necessário conforme cada finalidade específica.
- Celebração de contrato quando a pesquisa envolver o compartilhamento entre dois ou mais agentes de tratamento. Tais contratos podem estabelecer aspectos como papeis dos agentes de tratamento, finalidades do compartilhamento de dados, tipos de dados compartilhados, duração do tratamento, dentre outros.
- Sempre que possível, os dados devem ser anonimizados para reduzir os riscos de identificação dos indivíduos. Por isso, adote medidas como a remoção ou ocultação de informações que possam identificar diretamente os indivíduos.
- Quando não for possível a anonimização de dados, utilize outras medidas para garantir a segurança das informações e resguardar a identidade das pessoas, como técnicas de pseudonimização. Nestes casos, é possível a substituição de identificadores diretos por códigos ou pseudônimos, mantendo a possibilidade de reversão para casos necessários.
- Estabeleça os limites temporais adequados e proporcionais para o armazenamento de dados pessoais e informe o titular acerca dos critérios utilizados para a definição do período.
- Adote medidas técnicas e organizacionais seguras em seus sistemas e procedimentos, em atenção à segurança da informação contra divulgação acidental e perda ou destruição de dados de pesquisa. Exemplos de ações recomendadas envolvem a adoção da criptografia como padrão, definição de controle de acesso, e utilização de técnicas como a agregação de dados, desidentificação de dados e codificação de dados por chave.
- Avalie a necessidade de estabelecer critérios específicos de segurança conforme a categoria de dados pessoais envolvidos, para que as salvaguardas sejam distintas conforme a necessidade de proteção.

- Desenvolva um plano de pesquisa claro, que preveja as medidas de segurança de dados e garanta que o processamento esteja em conformidade com as leis aplicáveis. É recomendável que neste plano tenha a designação dos responsáveis pelo tratamento de dados pessoais, com a definição clara de responsabilidades de segurança durante a pesquisa; o contato do encarregado; e a indicação das pessoas responsáveis pela pesquisa.
- Avalie a necessidade de elaboração de documentos como o Relatório de Impacto à Proteção de Dados (RIPD), para garantir a identificação de eventuais riscos e a eficácia das medidas adotadas para a proteção de dados.
- Revise as medidas organizacionais das instituições envolvidas, com a celebração de acordos para compartilhamento de dados, reutilização de dados ou de transferência de materiais.
- Capacite os pesquisadores e equipes que manipulam os dados, para que possam seguir as melhores práticas de proteção de dados e estar cientes de suas responsabilidades em relação à confidencialidade e demais obrigações.
- Defina políticas claras e transparentes sobre as possibilidades de tratamento de dados, como os meios de compartilhamento, de armazenamento das informações e detalhes sobre possíveis usos futuros dos dados. As informações devem preferencialmente ser de fácil acesso aos titulares e disponíveis no local da coleta do consentimento.
- No caso de tratamento de dados de crianças e adolescentes, garanta que a atividade ocorra em respeito ao melhor interesse deste público e que, sempre que possível, os dados sejam anonimizados.
- Mantenha registros detalhados das práticas de proteção de dados adotadas, incluindo a concessão do consentimento livre, informado, inequívoco e destacado dos participantes e as medidas de segurança implementadas.
- No processo de divulgação dos resultados da pesquisa, garanta que a identidade dos participantes esteja resguardada.

Quando aplicável, também se exige dos projetos de pesquisa que observem aos padrões de qualidade reconhecidos e os processos necessários para a condução do trabalho. Ademais, em todas as pesquisas no campo da saúde, independente de envolveram o uso de dados pessoais, é necessário atentar-se aos padrões éticos e demais normas que regulem a temática a ser investigada. Dentre os princípios que devem ser observados, está o da privacidade (Art. 3º, VII; Art. 9º, III; Art. 17, IV, da Resolução CNS nº 510/2016). Ao analisar este aspecto, a ANPD apresentou algumas orientações, das quais se destacam:

PADRÕES ÉTICOS APLICÁVEIS A PESQUISAS

A conformidade com a LGPD não afasta a necessidade de respeitar as determinações de cunho ético ou de seguir os procedimentos próprios estabelecidos nas normas pertinentes.

Eventual dispensa do consentimento para os fins da LGPD, em razão da incidência de outra hipótese legal no caso concreto, não afasta a necessidade da obtenção do consentimento dos participantes de pesquisa, quando assim exigido pelas normas e padrões éticos aplicáveis.

É plenamente possível que o consentimento seja dispensável do ponto de vista da legislação de proteção de dados pessoais e necessário do ponto de vista ético.

O acesso a dados pessoais por instituições de ensino e respectivos pesquisadores é vinculado ao compromisso legal e ético de respeitar a confidencialidade desses dados e a privacidade dos titulares, bem como de utilizar esses dados apenas para a finalidade específica de realização de estudos e pesquisas.

Em decorrência dos padrões éticos vigentes e do princípio da boa-fé previsto na LGPD, o tratamento de dados pessoais para fins de estudos e pesquisas deve sempre se pautar por parâmetros de transparência, correção e lealdade, com a devida proteção à confiança e às legítimas expectativas dos titulares.

12.3 USO DE BIOMETRIA

A biometria é a análise técnica sobre pessoas, realizada através de "meios matemáticos e estatísticos, das características fisiológicas [...] ou comportamentais". Assim, são exemplos de técnicas de biometria:

BIOMETRIA: EXEMPLOS DE TÉCNICAS

Técnicas para identificação biométrica física ou fisiológica	• Verificação de impressão digital. • Análise de geometria e vascularização da mão. • Varredura da íris. • Análise da retina. • Reconhecimento de formato de orelha. • Reconhecimento facial.
Técnicas para identificação biométrica comportamental	• Reconhecimento de voz. • Análise de modo de andar. • Avaliação de assinaturas manuscritas. • Análise de pressionamento de teclas. • Análise de expressão facial.

No que se refere ao uso de imagens, o Conselho Europeu de Proteção de Dados (European Data Protection Board - EDPB) apresenta parâmetros que orientam a análise do processamento técnico e da intenção de identificar uma pessoa específica. Assim, imagens, por si só, não devem ser consideradas dados biométricos se não houver um processamento técnico destinado à identificação do indivíduo. A avaliação dessa situação exige não apenas uma análise cuidadosa por parte dos agentes de tratamento, mas também a documentação das ações e salvaguardas adotadas para proteger os direitos dos titulares.

No setor de saúde, há exemplos de uso dessas modalidades:

UTILIZAÇÃO DE BIOMETRIA NO SETOR DA SAÚDE

- Por prestadores de serviços de saúde e operadoras de planos de saúde para identificação de pacientes por meio de impressão digital, garantindo a prestação adequada de serviços (como exames) e a confirmação de identidade no acesso a aplicativos.
- Por prestadores de serviços de saúde para realização de triagem de pacientes e acesso à prontuários eletrônicos.
- Por fornecedores e distribuidores de produtos para saúde para prevenção de fraudes e roubo de identidade, utilizando técnicas de identificação biométrica física (reconhecimento facial ou de voz) e biométrica comportamental (análise de assinaturas manuscritas) para autenticação de funcionários para operação de certos equipamentos e rastreamento da responsabilidade de profissionais na produção de certos dispositivos.
- Pelas instituições do setor de saúde para redução de erros administrativos e clínicos, com controle de acesso a equipamentos e áreas físicas (de consultórios, salas administrativas, produção de equipamentos de saúde ou laboratórios) por meio de impressão digital e reconhecimento facial.

Independente das possibilidades de uso, os dados biométricos são considerados como dados pessoais sensíveis pela LGPD (Art. 5º, II). Por isso, os agentes de tratamento devem adotar maiores cautelas para resguardar a proteção de dados dos titulares, já que se verifica maior potencial discriminatório e de riscos contra os direitos dos titulares com a identificação biométrica.

Deve-se garantir o uso de dados estritamente necessários para a finalidade específica. O local e a forma de armazenamento das informações devem ser cuidadosamente selecionados, com controle, limitação e registro de acesso. Medidas como pseudonimização e criptografia são recomendadas para assegurar a segurança e integridade dos dados. Além disso, é essencial adotar medidas que garantam a confidencialidade, integridade e disponibilidade das informações, incluindo a detecção e prevenção de fraudes, bem como o armazenamento de dados brutos (como imagens faciais) separadamente de modelos biométricos. As estratégias de segurança devem ser continuamente aprimoradas à medida que a tecnologia evolui.

Especial atenção deve ser dada quando o tratamento de dados envolver grupos vulneráveis, como crianças, adolescentes ou idosos. No caso de menores, os agentes de tratamento são responsáveis por garantir que o uso dos dados ocorra exclusivamente para atender ao melhor interesse da criança ou adolescente. A análise dessas atividades relacionadas ao uso de biometria deve ser documentada para a elaboração do Relatório de Impacto à Proteção de Dados (RIPD) e auditoria.

Recomenda-se a elaboração de um RIPD, especialmente em casos de uso em larga escala. O documento deve incluir boas práticas e medidas

de segurança, tanto administrativas quanto técnicas, para prevenir e mitigar riscos. Além disso, as organizações devem implementar medidas adicionais, como controle de acesso físico e criptografia.

Por fim, as empresas devem garantir transparência em relação ao uso de dados pessoais para essas finalidades. Isso pode ser feito de forma proativa por meio da disponibilização de informações claras, compreensíveis e acessíveis em documentos institucionais, como políticas de privacidade, e em materiais informativos nos estabelecimentos, com avisos sobre o tratamento de dados e informações de contato para que os titulares possam exercer seus direitos.

12.4 UTILIZAÇÃO DE IA NA SAÚDE

O uso da IA no setor da saúde é bastante diversificado, podendo ser utilizado para melhorar o bem-estar e a qualidade de vida das pessoas, contemplando o desenvolvimento, treinamento e validação de algoritmos. Para tanto é necessária a garantia da proteção da privacidade dos titulares por meio da adoção de medidas que resguardem a integridade dos sistemas, além de mitigar os riscos de segurança cibernética.

BIOMETRIA: EXEMPLOS DE TÉCNICAS

Os **prestadores de serviços de saúde** podem, com apoio dos profissionais de saúde, utilizar ferramentas de IA para analisar exames de imagem (como radiografias, tomografias e ressonâncias magnéticas) e identificar anomalias, como tumores ou fraturas, com maior precisão e rapidez, auxiliando os médicos no diagnóstico.

As **operadoras de planos de saúde** podem utilizar sistemas de IA para identificar padrões anômalos de pedidos de reembolso ou faturamento, como auxílio ao processo de detecção de fraudes.

Os **fornecedores e distribuidores de produtos para saúde** podem utilizar sistemas de IA para otimizar rotas de distribuição e aumentar a eficiência na cadeia de suprimentos, garantindo que os produtos médicos cheguem aos prestadores de serviços de maneira eficaz, reduzindo custos logísticos e melhorando a entrega.

É essencial que essas iniciativas sejam transparentes, fornecendo aos titulares informações claras e suficientes sobre as tecnologias empregadas. Por isso, o uso da IA deve ser documentado desde o momento anterior à sua implementação, facilitando a consulta e a compreensão de aspectos pertinentes ao seu funcionamento. A transparência no uso de IA também promove a confiança dos usuários, permitindo que os indivíduos compreendam e, se necessário, contestem decisões que os afetam diretamente.

Para as atividades que envolvem a inteligência artificial, é possível indicar os seguintes princípios para orientar o seu uso no setor da saúde, estabelecidos pela Organização Mundial da Saúde (OMS):

PRINCÍPIOS PARA O USO DA IA NO SETOR DA SAÚDE CONFORME A ORGANIZAÇÃO MUNDIAL DA SAÚDE

- A IA deve proteger a autonomia humana, mantendo o controle das decisões médicas com os profissionais de saúde e garantindo a privacidade, confidencialidade e o consentimento informado adequado.
- O bem-estar, a segurança e o interesse público devem ser priorizados, com tecnologias de IA atendendo às exigências de segurança, precisão e eficácia, e com práticas de controle de qualidade implementadas.
- Transparência e explicabilidade são essenciais, com a documentação acessível antes da implantação da IA para facilitar a consulta pública e o debate sobre seu uso.
- A responsabilidade e a prestação de contas devem ser garantidas, com mecanismos de reparação para quem for prejudicado por decisões baseadas em algoritmos.
- Inclusão e equidade são necessárias, com IA projetada para evitar preconceitos e garantir acesso amplo e justo, considerando a diversidade do público-alvo.
- A IA deve ser responsiva e sustentável, com avaliações contínuas, minimizando impactos ambientais e promovendo capacitação para seu uso, incluindo no setor público.

Embora nem todos os sistemas de IA tratem dados pessoais, caso sejam utilizados dados pessoais as seguintes orientações podem ser adotadas:

ORIENTAÇÕES PARA PROTEÇÃO DE DADOS NA UTILIZAÇÃO E DESENVOLVIMENTO DE SISTEMAS DE IA

A aplicação da inteligência artificial na saúde oferece grandes oportunidades para inovação e melhoria na qualidade dos cuidados, mas também apresenta desafios relevantes, especialmente em relação à proteção de dados pessoais. Para enfrentar esses desafios, é essencial que as soluções de IA sejam desenvolvidas com um forte compromisso ético e em conformidade com a LGPD, assegurando que os direitos dos titulares sejam respeitados em todas as etapas.

- Capacitar as pessoas envolvidas no desenvolvimento e aplicação da IA garante supervisão adequada do uso e dos resultados.
- Estabelecer padrões claros de governança de dados em projetos de IA, detalhando a coleta, análise, armazenamento e as responsabilidades dos agentes envolvidos, como controlador e operador.
- Definir o propósito do uso da IA para atender aos princípios da finalidade e necessidade, evitando o tratamento de dados desnecessários (minimização).
- Documentar os objetivos específicos e justificados.
- Indicar a base legal para o tratamento de dados pessoais, garantindo conformidade com a LGPD, especialmente contra discriminação ilícita.
- Criar bancos de dados que sigam os parâmetros de legitimidade da LGPD, respeitando as condições de coleta de dados dos titulares.
- Adotar medidas de anonimização, pseudonimização ou restrição de visualização dos dados, sempre que possível.
- Estabelecer prazos de retenção e exclusão de dados pessoais proporcionais à finalidade do tratamento.
- Criar procedimentos periódicos de supervisão do uso da IA, acompanhando decisões automatizadas para garantir conformidade com a LGPD.
- Garantir que os titulares possam exercer seus direitos.
- Informar os titulares de maneira clara sobre as formas de uso dos dados pessoais através de políticas de privacidade de fácil compreensão, com detalhamento sobre os tipos de dados, finalidades e sistemas de IA envolvidos.
- Implementar práticas robustas de segurança da informação para prevenir incidentes, como acessos não autorizados. Exemplos que podem ser adotados: criptografia, autenticação de múltiplos fatores e sistemas de detecção de intrusões.
- Elaborar documentos de avaliação de impacto da IA, como a Avaliação de Impacto Algorítmico (AIA) e o Relatório de Impacto à Proteção de Dados (RIPD), conforme as diretrizes da LGPD e exigências da ANPD, para avaliação e mitigação de riscos.

ANEXO 1 - ARCABOUÇO NORMATIVO

Leis Federais

Lei nº 8.078, de 11 de setembro de 1990 - Dispõe sobre a proteção do consumidor.

Lei nº 8.080, de 19 de setembro de 1993 - Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências

Lei nº 9.656, de 3 de junho de 1998 - Dispõe sobre os planos e seguros privados de assistência à saúde.

Lei nº 9.782, de 26 de janeiro de 1999 - Define o Sistema Nacional de Vigilância Sanitária, cria a Agência Nacional de Vigilância Sanitária, e dá outras providências.

Lei nº 9.961 de 28 de janeiro de 2000 - Cria a Agência Nacional de Saúde Suplementar – ANS e dá outras providências.

Lei nº 12.965, de 23 de abril de 2014 – Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Lei nº 13.787, de 27 de dezembro de 2018 – Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.

Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

Lei nº 13.979, de 6 de fevereiro de 2020 - Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019.

Lei nº 14.063, de 23 de setembro de 2020 – Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos.

Lei nº 14.510, de 27 de dezembro de 2022 - Altera a Lei nº 8.080, de 19 de setembro de 1990, para autorizar e disciplinar a prática da telessaúde em todo o território nacional, e a Lei nº 13.146, de 6 de julho de 2015; e revoga a Lei nº 13.989, de 15 de abril de 2020.

Lei nº 14.198, de 2 de setembro de 2021 - Dispõe sobre videochamadas entre pacientes internados em serviços de saúde impossibilitados de receber visitas e seus familiares.

Lei nº 14.874, de 28 de maio de 2024 - Dispõe sobre a pesquisa com seres humanos e institui o Sistema Nacional de Ética em Pesquisa com Seres Humanos.

Resoluções Normativas e Súmulas Normativas da ANS

RN nº 137, de 20 de novembro de 2006 - Dispõe sobre as entidades de autogestão no âmbito do sistema de saúde suplementar.

RN nº 255, de 18 de maio de 2011 - Dispõe sobre a designação do responsável pelo fluxo das informações relativas à assistência prestada aos beneficiários de planos privados de assistência à saúde.

RN nº 305, de 9 de outubro de 2012 - Estabelece o Padrão obrigatório para Troca de Informações na Saúde Suplementar - Padrão TISS dos dados de atenção à saúde dos beneficiários dos Planos Privados de Assistência à Saúde.

RN nº 389, de 26 de novembro de 2015 - Dispõe sobre a transparência das informações no âmbito da saúde suplementar, estabelece a obrigatoriedade da disponibilização do conteúdo mínimo obrigatório de informações referentes aos planos privados de saúde no Brasil.

Súmula Normativa nº 27, de 10 de junho de 2015 – veda a prática de seleção de riscos pelas operadoras de planos de saúde na contratação de qualquer modalidade de plano privado de assistência à saúde.

RN nº 483, de 31 de março de 2022 - Dispõe sobre os procedimentos adotados pela Agência Nacional de Saúde Suplementar - ANS para a estruturação e realização de suas ações fiscalizatórias.

RN nº 489, de 29 de março de 2022 - Dispõe sobre a aplicação de penalidades para as infrações à legislação dos planos privados de assistência à saúde.

RN nº 501, de 31 de março de 2022 – Estabelece o Padrão obrigatório para Troca de Informações na Saúde Suplementar - Padrão TISS dos dados de atenção à saúde dos beneficiários de Plano Privado de Assistência à

Saúde; revoga as Resoluções Normativas nº 305, de 09 de outubro de 2012, e nº 341, de 27 de novembro de 2013.

RN nº 508, de 30 de março de 2022 - Dispõe sobre a suspensão dos Art. 12, § 2º, da Resolução Normativa nº 503, 30 de março de 2022, e 6º da Resolução Normativa nº 512, de 31 de março de 2022, para fins de cumprimento da decisão judicial proferida pelo Juízo da 2ª Vara Federal Cível da Seção Judiciária do Distrito Federal, nos autos da ação nº 0074233-60.2015.4.01.3400.

RN nº 531, de 4 de maio de 2022 - Dispõe sobre a definição, a segmentação e a classificação das Operadoras de Planos de Assistência à Saúde e revoga a Resolução de Diretoria Colegiada nº 39, de 27 de outubro de 2000, e a Resolução Normativa nº 315, de 28 de novembro de 2012.

RN nº 551, de 22 de novembro de 2022 - Dispõe sobre as normas para o envio de informações do Sistema de Informações de Produtos – SIP, para acompanhamento da assistência prestada aos beneficiários de planos privados de assistência à saúde e dá outras providências.

RN nº 559, de 30 de dezembro de 2022 - Dispõe sobre a transmissão dos arquivos, entre operadoras de planos privados de assistência à saúde e a Agência Nacional de Saúde Suplementar – ANS, das bases da Nota Técnica de Registro de Produto (NTRP), dos Comunicados de Reajustes de Planos Coletivos (RPC) e do Sistema de Informações de Produtos (SIP), por meio do Programa Transmissor de Arquivos - PTA.

Instrução Normativa nº 1/ANS, de 31 de março de 2022 - Regulamenta a Resolução Normativa nº 483, de 29, de março de 2022 no que tange aos procedimentos adotados pela Agência Nacional de Saúde Suplementar - ANS para a estruturação e realização de suas ações fiscalizatórias.

Resoluções da Diretoria Colegiada da Anvisa

RDC nº 14, de 5 de abril de 2011 - Institui o regulamento técnico com os requisitos para agrupamento de materiais de uso em saúde para fins de registro e cadastro na ANVISA e adota etiquetas de rastreabilidade para produtos implantáveis.

RDC nº 9, de 20 de fevereiro de 2015 - Dispõe sobre o Regulamento para a realização de ensaios clínicos com medicamentos no Brasil.

RDC nº 10, de 20 de fevereiro de 2015 - Dispõe sobre o regulamento para a realização de ensaios clínicos com dispositivos médicos no Brasil.

RDC Nº 305, de 24 de setembro de 2019 - Dispõe sobre requisitos para fabricação, comercialização, importação e exposição ao uso de dispositivos médicos personalizados.

RDC nº 556, de 30 de agosto de 2021 - Dispõe sobre os requisitos para agrupamento de materiais de uso em saúde para fins de registro e notificação na Agência Nacional de Vigilância Sanitária e adota etiquetas de rastreabilidade para produtos implantáveis.

RDC nº 824, de 26 de outubro de 2023 - Altera a Resolução de Diretoria Colegiada - RDC nº 786, de 5 de maio de 2023, que dispõe sobre os requisitos técnico-sanitários para o funcionamento de Laboratórios Clínicos, de Laboratórios de Anatomia Patológica e de outros Serviços que executam as atividades relacionadas aos Exames de Análises Clínicas (EAC) e dá outras providências.

Resoluções do CFM

Resolução CFM nº 1.605, de 15 de setembro de 2000 – Proíbe que o médico revele o conteúdo do prontuário ou ficha médica sem o consentimento do paciente.

Resolução CFM nº 1.638, de 9 de agosto de 2002 - Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde.

Resolução CFM nº 1.658, de 13 de dezembro de 2002 - Normatiza a emissão de atestados médicos, e dá outras providências.

Resolução CFM nº 1.821, de 23 de novembro de 2007 - Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde.

Resolução CFM nº 1.819, de 22 de maio de 2007 - Proíbe a inclusão do diagnóstico codificado (CID) ou tempo de doença no preenchimento das guias da TISS de consulta e solicitação de exames de seguradoras e operadoras de planos de saúde concomitantemente com a identificação do paciente.

Resolução CFM nº 1.851, de 14 de agosto de 2008 - Normatiza a emissão de atestados médicos e dá outras providências.

Resolução CFM nº 2.217, de 27 de setembro de 2018 – Código de Ética Médica.

Resolução CFM nº 2.107, de 17 de dezembro de 2014 - Define e normatiza a Telerradiologia.

Resolução CFM nº 2.299, de 30 de setembro de 2021 - Regulamenta, disciplina e normatiza a emissão de documentos médicos eletrônicos.

Resolução CFM nº 2.309, de 25 de março de 2022 - Estabelece regramento para publicização e compartilhamento de dados de médicos inscritos à luz da LGPD, do interesse público e das atribuições legais conferidas ao Conselho Médico.

Ministério da Saúde

Resolução nº CNS nº 218, de 06 de março de 1997 – Reconhece quais são os profissionais de saúde de nível superior.

Resolução CNS nº 251, de 07 de agosto de 1997 - Diretrizes e Normas Regulamentadoras de Pesquisa Envolvendo Seres Humanos.

Portaria CNS nº 1.820, de 13 de agosto de 2009 – Dispõe sobre os direitos e deveres dos usuários da saúde.

Resolução CNS nº 466, de 12 de dezembro de 2012 - Incorpora referenciais da bioética, tais como, autonomia, não maleficência, beneficência, justiça e equidade, dentre outros, e visa a assegurar os direitos e deveres que dizem respeito aos participantes da pesquisa, à comunidade científica e ao Estado.

Norma Operacional CONEP nº 001/2013 – Organização e funcionamento do Sistema CEP/CONEP, e sobre os procedimentos para submissão, avaliação e acompanhamento da pesquisa e de desenvolvimento envolvendo seres humanos no Brasil.

Portaria nº 589, de 20 de maio de 2015 - Institui a Política Nacional de Informação e Informática em Saúde (PNIIS).

Resolução CNS nº 506, de 3 de fevereiro de 2016 - Estabelece os critérios para o processo de acreditação de CEP do Sistema CEP/Conep, em instituições públicas e privadas. A tramitação do protocolo terá como base a gradação e a tipificação dos riscos definidas em norma própria, com critérios estabelecidos pela Comissão Nacional de Ética em Pesquisa (Conep), decorrentes das atividades de pesquisa envolvendo seres humanos.

Resolução CNS nº 510, de 07 de abril de 2016 - Dispõe sobre as normas aplicáveis a pesquisas em Ciências Humanas e Sociais cujos procedimentos metodológicos envolvam a utilização de dados diretamente obtidos com os participantes ou de informações identificáveis ou que possam acarretar riscos maiores do que os existentes na vida cotidiana, na forma definida nesta Resolução.

Portaria nº 2.022, de 7 de agosto de 2017 - Altera o Cadastro Nacional de Estabelecimentos de Saúde (CNES), no que se refere à metodologia de cadastramento e atualização cadastral, no quesito Tipo de Estabelecimentos de Saúde.

Portaria nº 467, de 20 de março de 2020 - Dispõe, em caráter excepcional e temporário, sobre as ações de Telemedicina, com o objetivo de regulamentar e operacionalizar as medidas de enfrentamento da emergência de saúde pública de importância internacional previstas no Art. 3º da Lei nº 13.979, de 6 de fevereiro de 2020, decorrente da epidemia de COVID-19.

Portaria MS/GS nº 1.434, de 28 de maio de 2020 - Institui o Programa Conecte SUS e altera a Portaria de Consolidação nº 1/GM/MS, de 28 de setembro de 2017, para instituir a Rede Nacional de Dados em Saúde e dispor sobre a adoção de padrões de interoperabilidade em saúde.

Portaria MS/GS nº 1.768, de 30 de julho de 2021 - Altera o Anexo XLII da Portaria de Consolidação GM/MS nº 2, de 28 de setembro de 2017, para dispor sobre a Política Nacional de Informação e Informática em Saúde (PNIIS).

REALIZAÇÃO: Instituto Consenso
DIAGRAMAÇÃO: Tiago Souto e Mateus Campos
JULHO_2026 • BRASÍLIA_DF