somos coop

CARTILHA
LGPD NA SAÚDE

2025

Unimed

PROTEÇÃO DE DADOS É PROTEÇÃO DE VIDAS

PRODUZIDA POR:

Carlos Henrique - chenrique@unimedfrutal.coop.br;

Sandra Garcia - gerencia@unimedfrutal.coop.br;

Jéssica S. Caetano - dpo@unimedfrutal.coop.br.

ANS - 37156-4

Unimed

somos coop

MUDE 1 HÁBITO

Esta cartilha visa orientar sobre como proteger a privacidade dos nossos beneficiários e garantir que a Unimed esteja em conformidade com a lei, fortalecendo a relação de confiança que é o pilar do nosso atendimento. Mais do que uma exigência jurídica, o zelo pelas informações de saúde é um compromisso ético: cada dado processado representa a vida e a intimidade de um paciente que confia em nossa marca.

Ao adotarmos as práticas aqui descritas, transformamos a proteção de dados em um padrão de excelência, assegurando que o cuidado com a segurança digital seja tão rigoroso quanto o cuidado médico prestado em nossas unidades.

ANS - 37156-4

SUMÁRIO:

ANS - 37156-4

Unimed

somos coop

DIRETORIA:

DIRETORIA EXECUTIVA E CONSELHO DE ADMINISTRAÇÃO (2024-2027):

Dr. Alberto Fuad Bichara - Presidente
Dr. Aliomar Alves Botelho - Diretor Financeiro
Dr. Marco Aurelio Miziara Morais - Diretor Administrativo
Dr. Carlos Alfredo Salci Queiroz - Conselheiro
Dr. Marcelo Palis Zago - Conselheiro

CONSELHO ETICO-TECNICO (2024-2027):

Dra. Maria Helena Diniz Afonso - Membro Efetivo
Dr. José Plínio dos Reis - Membro Efetivo
Dr. Luiz Maurício Afonso Reis - Membro Efetivo
Dr. Clarkson Alves Ferreira - Membro Suplente
Dra. Carmencita Pastori - Membro Suplente

CONSELHO FISCAL (2025):
Dr. Natal Henrique Lopes - Membro Efetivo
Dra. Adair Vieira de Lima Lisbôa - Membro Efetivo
Dr. Renan Ferreira - Membro Efetivo
Dra. karina Colado Dib - Membro Suplente
Dr. Lúcio Fernando Afonso -Membro Suplente

Aqui tem gente.

Aqui tem vida.

Aqui tem Unimed.

ANS - 37156-4

Unimed

FAZER JUNTO TRANSFORMA

Cooperar é fazer junto. E fazer junto transforma cuidado em conexão.

Transforma médicos cooperados, colaboradores e clientes em uma só comunidade.

Fazer junto transforma atendimento em acolhimento. Transforma cada ato em um compromisso com a vida.

Fazer junto transforma trabalho em propósito. Transforma mãos que cuidam em mão que constroem e protegem o futuro.

Fazer junto transforma um plano de saúde em um plano de vida. Transforma desafios em conquistas, inovação em bem-estar.

Fazer junto transforma união em presença de verdade. Transforma o cooperativismo em mais acesso, mais qualidade, mais saúde.

Transforma o agora em um legado para as próximas gerações.

Fazer junto transforma. E vai continuar transformando enquanto estivermos... JUNTOS!!

Aqui tem gente.

Aqui tem vida.

Aqui tem Unimed.

ANS - 37156-4

Unimed

QUEM SOMOS

Somos uma cooperativa de trabalho médico comprometida com o avanço sustentável do setor de saúde, por meio da prestação de serviços de alta qualidade, da geração de conhecimentos e da inovação das práticas assistenciais e de gestão. Para oferecer o melhor atendimento aos nossos clientes, contamos com médicos cooperados, profissionais dedicados à assistência, colaboradores na área administrativa e prestadores de serviço em saúde próprios e credenciados.

Moderna, sustentável e dinâmica. Essa é a Unimed Frutal que queremos: uma cooperativa cada vez mais consciente de sua responsabilidade e da importância do seu legado, preparada para enfrentar os desafios e cuidar da saúde de forma ética, transparente e inovadora.

Nosso Código de Conduta e Relacionamento está alinhado às demandas de um mundo em constante transformação e reforça nosso compromisso com um relacionamento ético e saudável com todos os nossos públicos.

NOSSOS VALORES:

- **Compromisso com os clientes**
- **Inovação contínua**
- **Qualidade com custo acessível**
- **Sustentabilidade econômica, social e ambiental**
- **Ética nos relacionamentos**

ANS - 37156-4

RESPONSABILIDADE SOCIAL

A Unimed Frutal se preocupa com o desenvolvimento sustentável da comunidade onde atua, com o respeito às pessoas e ao meio ambiente. A responsabilidade social é parte da nossa forma de conduzir os negócios, expressa em projetos junto às comunidades, mobilização de voluntários, acesso à cultura e cuidado com espaços públicos e ambientais.

PRINCÍPIOS DE RELACIONAMENTO

- Ética e respeito à legislação e contratos firmados com clientes
- Transparência nas informações e negociações
- Atendimento cordial, imparcial e profissional
- Sigilo e confidencialidade das informações dos clientes
- Respeito mútuo e valorização da empatia
- Clareza na comunicação, evitando termos técnicos excessivos

PRINCÍPIOS GERAIS DE CONDUTA

- Conformidade com leis nacionais e internacionais anticorrupção
- Proibição de fraude, corrupção, suborno, lavagem de dinheiro e sonegação fiscal
- Rejeição a vantagens indevidas, presentes ou favores que possam influenciar decisões
- Relacionamento íntegro com órgãos públicos
- Defesa de ambiente de trabalho digno, livre de assédio e discriminação
- Compromisso com a segurança da informação e proteção de dados (LGPD)

Unimed

INTRODUÇÃO

O cuidado com a saúde sempre foi o coração da Unimed. No entanto, no mundo conectado em que vivemos, cuidar de uma pessoa hoje também significa cuidar de seus dados. Informações sobre diagnósticos, exames, histórico familiar e até mesmo o endereço de nossos beneficiários são extensões de sua intimidade e dignidade.

Com a chegada da Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), o Brasil estabeleceu regras claras sobre como as empresas devem coletar, armazenar e utilizar informações pessoais. No setor de saúde, essa responsabilidade é ainda maior, pois lidamos com dados sensíveis, que exigem o mais alto nível de proteção e sigilo.

Esta cartilha foi desenvolvida para ser o seu guia prático. Ela visa orientar sobre como proteger a privacidade dos nossos beneficiários e garantir que a Unimed esteja em conformidade com a lei, transformando a segurança da informação em uma extensão do nosso ato de cuidar.

Ao proteger os dados de quem confia em nós, não estamos apenas cumprindo uma norma legal; estamos honrando nossa história e garantindo que o acolhimento Unimed aconteça tanto no consultório quanto no ambiente digital.

Unimed

LINHA DO TEMPO

2018 – PUBLICAÇÃO DA LEI

- 14 de agosto de 2018: A LGPD (Lei nº 13.709/2018) é sancionada e publicada no Diário Oficial da União.
- Inspirada no GDPR europeu, trouxe regras para coleta, uso e armazenamento de dados pessoais no Brasil

2019 – AJUSTES E CRIAÇÃO DA ANPD

- Alterações na lei para adequação ao cenário brasileiro.
- Criação da ANPD (Autoridade Nacional de Proteção de Dados), órgão responsável por regulamentar, fiscalizar e orientar a aplicação da LGPD

2020 – ENTRADA EM VIGÊNCIA

- 18 de setembro de 2020: LGPD entra oficialmente em vigor, após período de vacância de 18 meses.
- Empresas e instituições de saúde começam a se adequar às novas regras.

2021 – SANÇÕES ADMINISTRATIVAS

- Alterações na lei para adequação ao cenário brasileiro.
- Criação da ANPD (Autoridade Nacional de Proteção de Dados), órgão responsável por regulamentar, fiscalizar e orientar a aplicação da LGPD

2022 – CONSOLIDAÇÃO DA ANPD

- ANPD ganha autonomia técnica e administrativa.
- Início de regulamentações específicas para setores como saúde suplementar e telecomunicaçõe

Unimed

2023–2025 – EXPANSÃO E FISCALIZAÇÃO

Fiscalização e Guias da ANPD:

A ANPD vem ampliando sua atuação no setor de saúde com fiscalizações rigorosas e publicação de guias de boas práticas, exigindo das instituições não apenas o cumprimento formal da LGPD, mas a comprovação efetiva de controles técnicos e organizacionais. Isso inclui auditorias, pedidos de informações, termos de compromisso e sanções, além de orientações sobre bases legais, relatórios de impacto e padrões mínimos de segurança, tornando a conformidade um processo contínuo e verificável.

Dados Sensíveis na Saúde

Na saúde, dados como prontuários, exames, biometria e informações genéticas exigem proteção redobrada, pois seu uso indevido pode gerar discriminação e riscos graves ao paciente. Por isso, a LGPD determina controles rigorosos como criptografia, autenticação forte, restrição de acessos e transparência no uso, garantindo que cada dado seja tratado apenas para finalidades legítimas e com rastreabilidade clara.

Conformidade Contínua das Operadoras

Para operadoras como a Unimed, a conformidade com a LGPD não é um projeto pontual, mas um sistema permanente de governança. Isso envolve manter inventários de dados atualizados, realizar auditorias periódicas, treinar colaboradores, monitorar parceiros e responder rapidamente a incidentes. A prática contínua de segurança e transparência fortalece a confiança dos pacientes e protege a instituição contra riscos legais e reputacionais.

Além disso, a conformidade contínua exige que a operadora incorpore a cultura de proteção de dados em todas as áreas da organização. Isso significa que não apenas os setores jurídicos e de TI devem estar atentos, mas também equipes administrativas, médicas e de atendimento ao público. A integração da LGPD ao cotidiano da instituição garante que cada colaborador compreenda seu papel como guardião das informações dos pacientes, promovendo um ambiente de responsabilidade compartilhada. Dessa forma, a Unimed fortalece sua credibilidade, assegura a qualidade do serviço e demonstra compromisso com a ética e a privacidade na saúde.

Unimed

O QUE SÃO DADOS PESSOAIS E SENSÍVEIS?

No cotidiano da Unimed, lidamos com uma vasta quantidade de informações que definem a identidade e a vida de nossos beneficiários. O conceito fundamental da LGPD é o Dado Pessoal, que compreende qualquer informação capaz de identificar uma pessoa de forma direta ou indireta. Na prática, isso engloba desde os dados cadastrais básicos, como o nome completo, CPF e RG, até informações de contato como endereço, e-mail e número de telefone. Esses dados são a porta de entrada para o nosso atendimento e devem ser tratados com o devido zelo para garantir que a identidade do paciente permaneça protegida contra acessos não autorizados.

No entanto, o setor de saúde lida com uma categoria ainda mais restrita e protegida pela lei: o Dado Pessoal Sensível. Esta classificação abrange informações que tocam a intimidade mais profunda do indivíduo e que, se expostas, podem causar situações de discriminação ou vulnerabilidade. Para nós, isso inclui todo o histórico clínico, laudos de exames, prontuários, informações genéticas e até a biometria utilizada em nossos sistemas. Por serem dados que revelam o estado de saúde ou a vida sexual do paciente, a lei exige que o nosso rigor técnico e o nosso compromisso com o sigilo sejam elevados ao nível máximo de segurança.

Para que essa engrenagem de proteção funcione, a legislação define papéis claros para cada agente envolvido no processo. O Titular é a figura central, ou seja, o beneficiário que nos confia suas informações. A Unimed atua como Controladora, sendo a instituição responsável por tomar as decisões sobre como esses dados serão utilizados para garantir o melhor cuidado assistencial.

Quando contamos com o apoio de laboratórios ou clínicas parceiras para realizar exames, eles atuam como Operadores, processando os dados sob nossas orientações. Por fim, contamos com a figura do Encarregado de Dados (DPO), que atua como o guardião dessa conformidade, servindo de canal de comunicação entre o paciente, a Unimed e as autoridades reguladoras.

Unimed

NA SAÚDE, OS DADOS SENSÍVEIS EXIGEM PROTEÇÃO REDOBRADA!!

A proteção de dados sensíveis na área da saúde não é apenas uma exigência legal, mas um compromisso ético com a dignidade e a confiança dos pacientes. Informações como histórico médico, resultados de exames e dados genéticos representam muito mais do que registros administrativos: são fragmentos da vida de cada indivíduo, que precisam ser tratados com responsabilidade e sigilo. A LGPD estabelece diretrizes claras para garantir que esses dados sejam coletados e utilizados apenas para finalidades legítimas, evitando riscos de exposição indevida ou discriminação.

No contexto da Unimed Frutal, aplicar a LGPD significa fortalecer a relação de confiança entre pacientes e profissionais de saúde. Cada colaborador torna-se guardião de informações valiosas, e sua conduta impacta diretamente na credibilidade da instituição. Adotar boas práticas de segurança, transparência e respeito aos direitos dos titulares não apenas previne sanções legais, mas também reafirma o compromisso da cooperativa com a qualidade do cuidado e a proteção integral da vida.

Unimed

DADOS SENSIVEIS, QUAIS SÃO?

HISTÓRICO MÉDICO

O histórico médico reúne informações sobre doenças pré-existentes, tratamentos realizados, alergias e cirurgias. Esses dados são fundamentais para garantir um atendimento adequado, mas também podem expor vulnerabilidades do paciente se forem utilizados de forma indevida. Por isso, devem ser acessados apenas por profissionais autorizados e para fins estritamente relacionados ao cuidado em saúde.

DADOS GENÉTICOS

Os dados genéticos revelam características únicas de cada indivíduo, como predisposição a doenças hereditárias. Por serem altamente pessoais e impossíveis de alterar, exigem proteção máxima. O uso indevido pode gerar discriminação em seguros de saúde ou no mercado de trabalho, tornando essencial o cumprimento rigoroso da LGPD.

ANS - 37156-4

Unimed

DADOS SENSIVEIS, QUAIS SÃO?

DADOS BIOMÉTRICOS

Informações como impressões digitais, reconhecimento facial e padrões de voz são cada vez mais utilizados em sistemas de autenticação. Na saúde, podem ser aplicados para acesso a prontuários eletrônicos ou controle de entrada em áreas restritas. Por serem únicos e permanentes, precisam de medidas de segurança avançadas para evitar fraudes e acessos não autorizados.

SAÚDE MENTAL

Dados relacionados a diagnósticos psicológicos ou psiquiátricos são extremamente sensíveis, pois envolvem aspectos íntimos da vida emocional e comportamental do paciente. Vazamentos ou uso indevido podem gerar estigmatização e preconceito, reforçando a necessidade de confidencialidade absoluta.

Unimed

DADOS SENSIVEIS, QUAIS SÃO?

HÁBITOS DE VIDA

Informações sobre alimentação, prática de exercícios, consumo de álcool, tabaco ou medicamentos fazem parte do acompanhamento clínico. Embora pareçam simples, esses dados podem ser usados para traçar perfis de comportamento e até influenciar decisões de seguradoras. A LGPD garante que sejam tratados apenas para fins de promoção da saúde.

RESULTADOS DE EXAMES

Exames laboratoriais e de imagem revelam condições clínicas que, se divulgadas sem consentimento, podem comprometer a privacidade do paciente. O acesso deve ser restrito e controlado, assegurando que apenas profissionais envolvidos no tratamento possam consultá-los.

ANS - 37156-4

Unimed

DADOS SENSIVEIS, QUAIS SÃO?

RAÇA OU ETNIA

Informações sobre raça ou etnia são classificadas como sensíveis pela LGPD. Na saúde, podem aparecer em pesquisas ou prontuários e devem ser tratados com cautela para evitar discriminação

RELIGIÃO

Dados sobre crenças religiosas podem surgir em contextos de saúde (ex.: recusa de tratamentos). Devem ser respeitados e protegidos, sem uso para fins discriminatórios

VIDA SEXUAL

Dados sobre vida sexual ou saúde reprodutiva são extremamente íntimos. Vazamentos podem gerar constrangimento e discriminação, exigindo sigilo absoluto.

ANS - 37156-4

Unimed

COMO A ANS ADAPTOU NORMAS PARA OPERADORAS DE PLANOS

Cartilha LGPD na Saúde Suplementar

A ANS publicou uma cartilha oficial explicando como a LGPD deve ser aplicada no setor de saúde suplementar.

O documento orienta operadoras sobre coleta, armazenamento e compartilhamento de dados pessoais e sensíveis, reforçando princípios como finalidade, necessidade e segurança

Resolução Normativa nº 623/2024

A norma que entrou em vigor em julho de 2025 trouxe uma transformação significativa no relacionamento entre operadoras de planos de saúde e seus beneficiários. O objetivo central foi garantir maior agilidade no atendimento, permitindo que as demandas dos usuários fossem tratadas de forma rápida e eficiente. Além disso, estabeleceu mecanismos de rastreabilidade das informações e solicitações, assegurando que cada interação pudesse ser acompanhada e documentada, o que fortalece a confiança e a transparência entre pacientes e operadoras.

Outro ponto essencial foi a ênfase na transparência da comunicação e na resolução de problemas, criando um ambiente em que os beneficiários têm clareza sobre seus direitos e sobre os processos internos das operadoras. A norma também introduziu um modelo de fiscalização responsiva, voltado para a prevenção de falhas e incentivo às boas práticas, em vez de apenas punir irregularidades. Esse enfoque promove uma cultura de conformidade contínua, estimulando as operadoras a adotarem padrões elevados de governança e proteção de dados, especialmente no setor de saúde suplementar.

ANS - 37156-4

Unimed

COMO A ANS ADAPTOU NORMAS PARA OPERADORAS DE PLANOS

Padrão TISS

A ANS centralizou a coleta de informações assistenciais no padrão TISS, substituindo sistemas anteriores como o SIP.

Isso exige ajustes tecnológicos das operadoras para garantir interoperabilidade e segurança na troca de dados entre hospitais, clínicas e laboratórios

Impacto direto para Unimed

A governança contínua é essencial para garantir que o tratamento de dados esteja sempre em conformidade com a LGPD. Isso significa manter inventários atualizados de todas as informações coletadas, realizar auditorias periódicas e elaborar relatórios de impacto sempre que novos processos forem implementados. Dessa forma, a instituição consegue identificar riscos, corrigir falhas e demonstrar responsabilidade perante pacientes e órgãos reguladores.

A segurança reforçada envolve a adoção de medidas técnicas robustas para proteger dados sensíveis. Entre elas estão a criptografia para armazenamento e transmissão de informações, autenticação forte para acesso aos sistemas e controle rigoroso de quem pode consultar prontuários eletrônicos. Essas práticas reduzem a possibilidade de vazamentos e garantem que apenas profissionais autorizados tenham acesso às informações médicas.

A transparência com beneficiários fortalece a confiança e assegura que os pacientes conheçam seus direitos. Isso inclui disponibilizar canais claros e acessíveis para solicitações de acesso, correção ou exclusão de dados pessoais. Ao oferecer comunicação direta e transparente, a operadora demonstra respeito à privacidade e reforça seu compromisso ético com os titulares das informações.

Por fim, a fiscalização ativa realizada pela ANS e pela ANPD garante que as práticas das operadoras sejam constantemente monitoradas. Caso haja descumprimento das normas, podem ser aplicadas sanções administrativas e financeiras, além da exigência de ajustes imediatos nos processos. Esse controle externo assegura que a proteção de dados seja tratada como prioridade e não apenas como obrigação formal.

Unimed

DIREITOS DOS TITULARES:

- **Confirmação da existência de tratamento: o titular pode perguntar se seus dados estão sendo tratados.**
- **Acesso aos dados: direito de saber quais informações estão sendo coletadas e usadas.**
- **Correção: atualização de dados incompletos ou incorretos.**
- **Anonimização, bloqueio ou eliminação: quando os dados forem excessivos ou tratados em desconformidade.**
- **Portabilidade: transferência dos dados para outro fornecedor de serviço ou produto.**
- **Eliminação dos dados: quando o consentimento for retirado, salvo exceções legais.**
- **Informação sobre compartilhamento: saber com quem seus dados foram compartilhados.**
- **Revogação do consentimento: o titular pode mudar de ideia a qualquer momento.**
- **Petição à ANPD: possibilidade de reclamar diretamente à Autoridade Nacional de Proteção de Dados.**
- **Oposição ao tratamento: recusar usos específicos de seus dados.**

CONSENTIMENTO:

- **O consentimento, no âmbito da Lei Geral de Proteção de Dados (LGPD), é entendido como uma manifestação livre, informada e inequívoca do titular, concedida para uma finalidade específica. Ele deve ser apresentado de forma clara e acessível, garantindo que o indivíduo compreenda plenamente como seus dados serão utilizados e para quais objetivos. Além disso, o consentimento não é definitivo: o titular possui o direito de revogá-lo a qualquer momento, reforçando sua autonomia e controle sobre as próprias informações pessoais.**

- **Entretanto, é importante destacar que o consentimento não é absoluto. A LGPD prevê hipóteses em que o tratamento de dados pode ocorrer independentemente da autorização do titular, como nos casos de cumprimento de obrigação legal, proteção da vida ou da saúde, ou ainda na execução de políticas públicas. Essas exceções demonstram que, embora o consentimento seja um pilar essencial da proteção de dados, existem situações em que o interesse coletivo ou a necessidade legal se sobrepõem à vontade individual.**

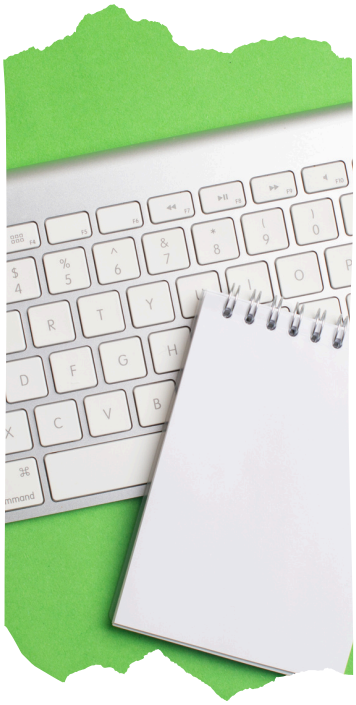
ANS - 37156-4

Unimed

AGENTES DE TRATAMENTO:

- **O controlador é a pessoa física ou jurídica responsável por tomar as decisões sobre o tratamento de dados pessoais. Cabe a ele definir a finalidade para a qual os dados serão utilizados e os meios empregados nesse processo. Em outras palavras, o controlador estabelece o "porquê" e o "como" do tratamento, assumindo a posição de autoridade principal na gestão das informações, além de responder diretamente pela conformidade com a Lei Geral de Proteção de Dados (LGPD).**

- **O operador, por sua vez, é a entidade ou pessoa que realiza o tratamento de dados em nome do controlador, seguindo suas instruções. Ele não possui autonomia para decidir sobre a finalidade ou os meios do tratamento, atuando de forma subordinada às diretrizes estabelecidas pelo controlador. Sua função é executar as atividades técnicas e administrativas necessárias para que o tratamento ocorra conforme determinado, garantindo que as operações estejam alinhadas às exigências legais.**



- **Tanto controlador quanto operador possuem responsabilidades conjuntas e devem observar os princípios fundamentais da LGPD. Isso inclui respeitar a finalidade do tratamento, garantindo que os dados sejam usados apenas para o propósito informado; assegurar a adequação, ou seja, que o uso dos dados esteja compatível com o contexto da coleta; aplicar o princípio da necessidade, limitando o tratamento apenas ao que for estritamente necessário; adotar medidas de segurança para proteger os dados contra acessos indevidos ou vazamentos; agir de forma preventiva para evitar riscos e danos; e, finalmente, garantir que não haja discriminação no uso das informações pessoais. Esses princípios formam a base ética e legal da proteção de dados no Brasil.**

- **Exemplo: Na prática, a Unimed Frutal atua como controladora, pois coleta e administra os dados dos beneficiários, definindo a finalidade e os meios de uso dessas informações para garantir atendimento médico e gestão do plano de saúde, sendo responsável pela conformidade com a LGPD. Já a clínica ou laboratório credenciado exerce o papel de operador, utilizando os dados apenas para realizar o atendimento ou exame solicitado, sem autonomia para outras finalidades, seguindo as instruções da Unimed e adotando medidas de segurança como prontuário eletrônico protegido e acesso restrito.**

Unimed

ENCARREGADO DE DADOS (DPO)

- O encarregado de dados pessoais, também conhecido como DPO (Data Protection Officer), é definido pela Lei Geral de Proteção de Dados (LGPD), em seu artigo 5º, inciso VIII, como a pessoa física ou jurídica designada para atuar como elo de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Essa função é estratégica dentro das organizações, pois garante que exista uma figura responsável por mediar interesses, esclarecer dúvidas e assegurar que os direitos dos titulares sejam respeitados, ao mesmo tempo em que promove a conformidade legal no tratamento das informações pessoais.

- Entre suas principais funções, o encarregado deve receber reclamações e comunicações dos titulares de dados, servindo como ponto de contato direto para que os indivíduos possam exercer seus direitos previstos na LGPD. Além disso, cabe a ele orientar funcionários e contratados da organização sobre práticas adequadas de proteção de dados, disseminando a cultura de privacidade e segurança da informação. Outra atribuição essencial é a interação com a ANPD, fornecendo informações, relatórios e esclarecimentos sempre que solicitado, de modo a garantir que a empresa esteja alinhada às exigências regulatórias e às boas práticas de governança em dados pessoais.

- No que diz respeito às responsabilidades, é importante destacar que o DPO não é considerado um agente de tratamento, ou seja, não toma decisões sobre a finalidade ou os meios do uso dos dados. Sua atuação é mais voltada ao aconselhamento e à supervisão, funcionando como um conselheiro especializado. No entanto, isso não significa que esteja isento de responsabilidades: o encarregado pode ser responsabilizado caso haja negligência, imprudência ou dolo em suas atividades, especialmente se sua conduta resultar em prejuízos para titulares ou para a própria organização.

- Por fim, para desempenhar esse papel de forma eficaz, o encarregado deve possuir conhecimento jurídico e técnico sobre proteção de dados, além de compreender os princípios da segurança da informação e da gestão de riscos. Essa combinação de competências é fundamental para que o DPO consiga orientar a empresa na implementação de políticas de privacidade, identificar vulnerabilidades e propor medidas preventivas, consolidando a confiança entre a organização, os titulares e os órgãos reguladores.

ANS - 37156-4

RESPONSABILIDADES:

A ANS, como reguladora da saúde suplementar, adaptou suas normas para reforçar a responsabilidade das operadoras na proteção de dados dos beneficiários. Ela exige rastreabilidade das informações, transparência na comunicação e agilidade no atendimento às demandas dos usuários, além de fiscalizar continuamente as práticas das operadoras. Caso haja descumprimento, a ANS pode aplicar sanções administrativas, exigir ajustes imediatos e até suspender atividades, garantindo que a proteção de dados seja tratada como parte essencial da qualidade do serviço.

As operadoras de saúde suplementar, como a Unimed, têm responsabilidade direta em implementar programas de governança em privacidade, manter inventários de dados atualizados, realizar auditorias periódicas e treinar colaboradores. Também devem assegurar que parceiros e prestadores de serviço sigam os mesmos padrões de proteção. Essa responsabilidade vai além da conformidade legal: envolve proteger a confiança dos pacientes, garantir sigilo médico e demonstrar compromisso ético com a privacidade e a dignidade humana.

A LGPD estabelece que controladores e operadores de dados são responsáveis por garantir que o tratamento das informações pessoais e sensíveis seja feito de forma segura, transparente e dentro da legalidade. Isso significa que qualquer instituição que coleta ou utiliza dados deve adotar medidas técnicas e administrativas para prevenir incidentes, além de responder civil, administrativa e até criminalmente em caso de uso indevido ou vazamento. A responsabilidade é objetiva: mesmo sem intenção, a empresa pode ser responsabilizada se houver falha na proteção.

RESPONSABILIDADES:

O controlador e o operador podem ser responsabilizados por danos materiais e morais decorrentes de um tratamento irregular de dados pessoais. Isso significa que, caso haja violação das normas da LGPD ou uso inadequado das informações, ambos podem ser chamados a responder judicialmente pelos prejuízos causados aos titulares, reforçando a importância da conformidade e da adoção de boas práticas de proteção de dados.

Em determinadas situações, a lei prevê a responsabilidade solidária entre controlador e operador. Isso ocorre, por exemplo, quando o operador descumpre instruções lícitas fornecidas pelo controlador ou quando ambos participam de forma conjunta em práticas que resultam em violação da legislação. Nesses casos, os dois agentes respondem juntos, garantindo maior proteção ao titular e assegurando que a reparação dos danos seja efetiva.

A LGPD também estabelece excludentes de responsabilidade no artigo 43. Entre elas, estão os cenários em que o agente de tratamento não participou do processo questionado, quando não houve violação da lei, ou ainda quando o dano decorreu de culpa exclusiva do titular ou de terceiros. Essas hipóteses funcionam como mecanismos de defesa, permitindo que o controlador ou operador se isente de responsabilidade caso comprovem que não contribuíram para o prejuízo.

Por fim, o artigo 46 da LGPD reforça a obrigação de adoção de medidas de segurança técnicas e administrativas para proteger os dados pessoais. Isso inclui práticas como controle de acesso, criptografia, políticas internas de segurança da informação e treinamentos periódicos para colaboradores. A implementação dessas medidas é essencial para reduzir riscos de vazamentos, acessos indevidos ou qualquer forma de tratamento inadequado, demonstrando o compromisso da organização com a privacidade e a proteção dos dados.

ANS - 37156-4

Unimed

RESPONSABILIDADE OBJETIVA NO CÓDIGO CIVIL:

O Código Civil (art. 927, parágrafo único) estabelece que haverá responsabilidade objetiva quando a atividade normalmente desenvolvida pelo autor do dano implicar risco para os direitos de terceiros. No setor de saúde, o tratamento de dados sensíveis é considerado uma atividade de risco, pois envolve informações íntimas e de grande impacto sobre a vida dos pacientes. Assim, operadoras como a Unimed devem responder pelos danos causados, independentemente de culpa, sempre que houver falha na proteção ou uso indevido dos dados. Essa responsabilidade objetiva reforça a necessidade de governança contínua, já que o risco é inerente à atividade e a obrigação de proteger é permanente.

O art. 927, parágrafo único, do Código Civil dispõe que haverá responsabilidade objetiva quando a atividade normalmente desenvolvida pelo autor do dano implicar risco para os direitos de terceiros. Isso significa que, em atividades de risco, como o tratamento de dados sensíveis na saúde, não é necessário provar culpa: basta demonstrar o dano e o nexo causal.

Vazamento de prontuários eletrônicos: se um sistema da operadora sofre falha de segurança e expõe diagnósticos de pacientes, a responsabilidade é objetiva. O paciente não precisa provar que houve negligência, apenas que o vazamento ocorreu e lhe causou dano.

Compartilhamento indevido de exames: caso um colaborador envie resultados de exames para terceiros sem autorização, a operadora responde objetivamente, pois o risco é inerente à atividade de tratar dados sensíveis.

ANS - 37156-4

Unimed

DIREITOS DOS TÍTULARES:

O primeiro direito assegurado pela LGPD é o acesso aos dados. Isso significa que o paciente pode solicitar à Unimed informações sobre quais dados pessoais e sensíveis estão armazenados e como estão sendo utilizados. Na prática, um beneficiário pode pedir uma cópia de seu prontuário eletrônico ou verificar quais dados cadastrais constam no sistema. Esse acesso deve ser fornecido de forma clara, segura e em linguagem compreensível, reforçando a transparência da instituição.

Outro direito fundamental é a correção de dados. Caso o paciente identifique informações incorretas ou desatualizadas, como endereço, telefone ou até mesmo dados clínicos, ele pode solicitar a atualização imediata. A Unimed deve garantir que esses ajustes sejam feitos com agilidade, evitando problemas futuros no atendimento ou na comunicação com o beneficiário. Esse processo demonstra cuidado e responsabilidade com a integridade das informações.

A LGPD também assegura o direito à exclusão de dados. Isso ocorre quando informações não são mais necessárias para a finalidade original ou estão sendo tratadas sem base legal adequada. Por exemplo, um ex-beneficiário pode solicitar a exclusão de dados que não precisam ser mantidos após o término do contrato. A Unimed deve avaliar cada caso, respeitando os prazos legais de guarda, mas garantindo que dados desnecessários sejam eliminados para proteger a privacidade do paciente.

Outro ponto importante é a portabilidade de dados, que permite ao paciente transferir suas informações para outra operadora ou instituição de saúde. Se um beneficiário decide migrar para outro plano, pode solicitar que seus dados cadastrais e históricos sejam enviados de forma estruturada e segura. Esse direito garante autonomia ao paciente e promove concorrência saudável entre operadoras, já que facilita a transição sem perda de informações relevantes.

Exemplo prático:

Imagine que um paciente esteja em tratamento de uma doença crônica e decida mudar de plano de saúde. Com a portabilidade:

- **Seu histórico de consultas e exames é transferido automaticamente.**
- **O novo médico tem acesso imediato às informações, evitando atrasos ou retrabalho.**
- **O paciente mantém a linha de cuidado contínua, sem riscos de falhas por falta de dados.**

Unimed

BOAS PRÁTICAS NO DIA A DIA:

SENHAS FORTES

O uso de senhas fortes é essencial para proteger informações pessoais e corporativas. Uma senha considerada segura deve conter letras maiúsculas e minúsculas, números e caracteres especiais, além de evitar dados óbvios como datas de nascimento ou nomes próprios. Complementarmente, o bloqueio automático da tela em computadores e celulares impede acessos indevidos quando o dispositivo fica sem supervisão, reduzindo riscos de exposição de dados.

DESCARTE SEGURO

Documentos impressos que contenham informações sensíveis não devem ser descartados no lixo comum. O ideal é utilizar fragmentadoras de papel ou serviços especializados em destruição de documentos, garantindo que dados confidenciais não possam ser recuperados. Essa prática evita que terceiros tenham acesso a informações estratégicas ou pessoais.

EVITAR COMPARTILHAMENTO

Dados corporativos ou informações confidenciais nunca devem ser enviados por aplicativos de mensagens ou e-mails pessoais, pois esses canais não oferecem o mesmo nível de segurança que sistemas corporativos. O uso de plataformas oficiais e autorizadas garante maior proteção contra interceptações e vazamentos.

EXEMPLOS DE CONDUTAS

- Criar senhas complexas e atualizá-las periodicamente.
- Bloquear a tela ao se ausentar do computador.
- Utilizar fragmentadora para descartar documentos sensíveis.
- Compartilhar informações apenas em sistemas corporativos autorizados.
- Habilitar autenticação multifator (MFA): além da senha, usar um segundo fator como código no celular ou aplicativo de autenticação.
- Manter softwares e sistemas atualizados: instalar sempre as atualizações de segurança para reduzir vulnerabilidades.
- Evitar uso de redes Wi-Fi públicas sem proteção: quando necessário, utilizar VPN para garantir a segurança da conexão.
- Organizar documentos físicos em locais seguros: guardar arquivos confidenciais em armários trancados ou áreas restritas.

ANS - 37156-4

Unimed

FLUXO DE ATENDIMENTO SEGURO:

Os dados do paciente percorrem um fluxo contínuo que começa no cadastro e segue por consulta, exames e faturamento. Em cada etapa, há diferentes sistemas, pessoas e documentos envolvidos. Mapear claramente quem acessa o quê e por qual meio (sistema, planilha, papel, e-mail) é essencial para reduzir riscos e manter conformidade.

CADASTRO

Nesta etapa são coletados os dados pessoais e de saúde do paciente, que devem ser registrados apenas em sistemas oficiais e protegidos por controles de acesso. O ponto crítico é evitar o uso de planilhas locais ou exposição de informações em balcões de atendimento.

CONSULTA

Durante a consulta, informações clínicas são inseridas no prontuário eletrônico. É fundamental que apenas profissionais autorizados tenham acesso e que os registros sejam feitos exclusivamente no sistema oficial. O risco está em anotações fora do sistema ou em dispositivos sem bloqueio de tela.

EXAMES

Os dados do paciente são compartilhados com laboratórios ou serviços de imagem para realização de exames. O cuidado principal é garantir que esse compartilhamento ocorra por canais seguros e criptografados, evitando envio por e-mails pessoais ou mídias não protegidas.

FATURAMENTO

Na fase de cobrança, apenas os dados estritamente necessários devem ser utilizados e enviados às operadoras por sistemas homologados. O ponto crítico é evitar transmissões sem criptografia ou retenção prolongada de informações além do prazo legal.

ATENÇÃO GERAL

Em todas as etapas, é essencial aplicar controles de acesso, autenticação forte, criptografia e descarte seguro de documentos físicos. Treinamento contínuo das equipes e uso exclusivo de sistemas corporativos reduzem falhas de segurança e riscos de vazamento de dados.

Unimed

PONTOS DE REFLEXÃO:

A maturidade em proteção de dados não é um estado, é um processo contínuo que exige autonomia real e conhecimento multidisciplinar do DPO. Quando o encarregado possui independência para apotar riscos, priorizar ações e influenciar decisões, ele transforma políticas em práticas vivas: integra jurídico, tecnologia, segurança da informação, processos e pessoas. Essa visão sistêmica garante que a privacidade esteja incorporada desde o desenho das iniciativas (privacy by design e by default), com métricas claras, revisões periódicas e capacidade de resposta ágil a incidentes e demandas dos titulares.

A responsabilização na LGPD dialoga com outros microssistemas legais, como o Código de Defesa do Consumidor, o Marco Civil da Internet e normas setoriais. Essa conexão amplia o escopo de deveres e a exigência de diligência, exigindo que controladores e operadores mantenham documentação robusta (registros de tratamento, políticas, relatórios de impacto), governança contratual com terceiros e evidências de medidas técnicas e administrativas eficazes. Em um ambiente regulatório dinâmico, conformidade passa a ser um ciclo de melhoria contínua: monitorar atualizações da ANPD, revisar bases legais, reduzir excessos de dados, reforçar controles e testar planos de resposta a incidentes.

Mais que conformidade, a cultura de proteção de dados é o alicerce da confiança entre empresas e titulares. Confiança nasce de transparência, previsibilidade e respeito: avisos de privacidade claros, canais acessíveis, atendimento célere aos direitos, segurança prática no dia a dia e prestação de contas sobre decisões automatizadas e compartilhamentos. Ela se sustenta em hábitos como : treinamentos recorrentes, auditorias internas, avaliação de fornecedores, revisão de processos e indicadores de risco. E se prova nos momentos críticos, quando a organização comunica com clareza, mitiga impactos e aprende com o que aconteceu.

A continuidade se traduz em governança viva: ciclos regulares de avaliação (PDCA), metas e indicadores de privacidade, integração com gestão de riscos corporativos, e um DPO com assento estratégico para influenciar prioridades e investimentos. Assim, a proteção de dados deixa de ser um projeto com início e fim e se torna uma competência organizacional permanente, capaz de adaptar-se ao negócio, à tecnologia e à regulação, mantendo os direitos dos titulares no centro e a confiança como resultado sustentado.

Unimed

BIBLIOGRAFIA:

- BRASIL. Constituição da República Federativa do Brasil de 1988.
- BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).
- BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Código Civil.
- BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor.
- BRASIL. Lei nº 8.112, de 11 de dezembro de 1990. Estatuto dos Servidores Públicos Federais.
- BRASIL. Lei nº 8.429, de 2 de junho de 1992. Lei de Improbidade Administrativa.
- BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação.
- AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Site oficial da ANPD.
- EUROPEAN DATA PROTECTION BOARD (EDPB). Site oficial do EDPB.

- AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Site oficial da ANPD.
- EUROPEAN DATA PROTECTION BOARD (EDPB). Site oficial do EDPB
- GRAN FACULDADE. Apostila – Reparação de Danos e as Sanções Administrativas. Professor(a): Núbia de Paula.
- GRAN FACULDADE. Apostila – Instituições Jurídicas e Administrativas no Contexto do Tratamento de Dados. Professor(a): Núbia de Paula.