

Levando em conta:

- I A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709 de 2018 e sua ampla repercussão na vida do Sistema Unimed;
- II A existência de uma norma geral do Sistema Unimed, a Norma Derivada nº 15 de 2019, da Unimed do Brasil (anexa), que estabelece regras gerais em relação à matéria, com validade sistêmica universal; e
- III A necessidade de uma unidade de conduta no trato da matéria, dado que a eventual prática irregular, ou fora dos padrões, de uma Unimed pode gerar danos a todo o Sistema, com ressarcimento integral pela responsável, conforme consta da Norma Derivada nº 15;

o Conselho de Administração da Unimed Federação/RS, com a competência que lhe outorga o art. 48, inciso II, do Estatuto da Entidade, EXPEDE a

NORMA DERIVADA Nº 02

regramento estadual da política estadual de proteção de dados pessoais

CAPÍTULO I CONCEITOS

1.1. Para os fins aspirados pela presente Norma, são considerados:

1.1.1. “DADO PESSOAL”: informação relacionada à pessoa natural identificada ou identificável.

1.1.2. “DADO PESSOAL SENSÍVEL”: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

1.1.3. “TRATAMENTO”: qualquer operação ou conjunto de operações efetuadas sobre dados pessoais ou sobre conjunto de dados pessoais, por meio automatizado ou não automatizado, tais como a coleta, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, a exclusão ou a destruição.

1.1.4. “TITULAR DE DADOS PESSOAIS”: pessoa física que tenha seus dados pessoais tratados pelo Sistema Cooperativo Unimed, independentemente de relação pretérita, atual ou futura com o Sistema, podendo ser, mas não se limitando a consumidor, colaborador, parceiro comercial entre outras pessoas físicas.

1.1.5. “CONTROLADOR”: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

1.1.6. “OPERADOR”: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

1.1.7. “ENCARREGADO”: pessoa indicada pelo Controlador e Operador – conforme obrigatoriedade pautada em lei – para atuar como canal de comunicação entre o agente de tratamento, os Titulares de Dados Pessoais e a Autoridade Nacional de Proteção de Dados.

1.1.8. “AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS”: Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais.

1.1.9. “BASE LEGAL”: hipótese legal que autoriza o tratamento de dados pessoais.

1.1.10. “RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD”: 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, as medidas, as salvaguardas e os mecanismos de mitigação de risco.

1.1.11. “COMITÊ ESTADUAL DE GESTÃO DE PRIVACIDADE”: estrutura Federativa vinculada à Diretoria da Unimed Federação/RS, com a finalidade de coordenar, disseminar, organizar e desenvolver a padronização das ações de governança relacionadas ao Programa de adequação à LGPD junto às Cooperativas do Sistema Unimed do Estado do Rio Grande do Sul e às entidades por elas constituídas.

1.1.12. “COMITÊ LOCAL DE PRIVACIDADE”: estrutura estabelecida por cada Unimed do Estado e as entidades por elas constituídas, composta por um Diretor ou Responsável Legal, Encarregado de Dados Pessoais (este devendo ser convocado para tanto), Coordenador do Comitê Local de Privacidade, bem como, demais colaboradores convidados para multiplicar, desenvolver e implantar a adequação à LGPD junto às suas unidades, como também pela proteção, mapeamento e registro de tratamento dos dados pessoais recebidos das coirmãs.

1.1.13. “ESCRITÓRIO ESTADUAL DE PRIVACIDADE E SEGURANÇA”: estrutura Federativa composta por Encarregado pelo Tratamento de Dados Pessoais do Projeto Estadual, Assessores e Consultores Técnicos para multiplicar, suportar e auditar a adequação à LGPD de forma sistêmica e rotineira, conforme esta Norma.

CAPÍTULO II PRINCÍPIOS, VALORES E ESCOPO

Art. 1º A privacidade e a proteção da privacidade dos dados pessoais dos titulares destes é valor primordial do Sistema Cooperativo Unimed.

Art. 2º Todo e qualquer tratamento de dados pessoais que seja realizado no âmbito do Sistema Cooperativo Unimed deverá contar com finalidade legítima e específica, bem como, estar amparado em uma das bases legais previstas na LGPD.

Art. 3º É vedado o tratamento de dados pessoais para fins discriminatórios.

Art. 4º Cada Unimed deverá ser responsável pela proteção, mapeamento e registro de tratamento dos dados pessoais recebidos entre o conjunto das Cooperativas do Sistema Unimed do Estado do Rio Grande do Sul e as entidades por elas constituídas.

Parágrafo único: Também é da responsabilidade de cada Unimed do Estado o trato dos dados das cooperativas de âmbito nacional do Sistema Unimed de acordo com as regras da Unimed do Brasil.

Art. 5º Todos que estiverem sob a égide da presente política deverão implementar meios para conferir aos titulares a transparência necessária em relação ao uso de seus dados pessoais, no que tange à finalidade, forma e duração do tratamento, identificação e informações de contato do Encarregado, informações acerca do uso compartilhado, responsabilidades dos agentes envolvidos e direitos dos titulares.

Parágrafo único: Decorre dos deveres previstos no caput deste artigo a necessidade de estabelecimento, ou obediência àqueles regulamentos vigentes, que sejam efetivos para atendimento dos direitos dos titulares tais como, exemplificativamente, acesso, retificação, portabilidade, exclusão, bloqueio e revogação de consentimento.

Art. 6º Todo tratamento de dados pessoais realizado no âmbito do Sistema Cooperativo Unimed deverá atender ao princípio da necessidade, sendo vedado qualquer excesso.

Art. 7º Cada Unimed tem a responsabilidade de implementar os meios tecnológicos e de processos operacionais que cumpram os critérios mínimos de segurança na proteção de dados sensíveis de saúde dos beneficiários próprios e do conjunto das Cooperativas do Sistema Unimed do Estado do Rio Grande do Sul e entidades por elas constituídas.

Art. 8º Deverá ser institucionalizada pelo Sistema Estadual de Proteção de Dados (SEPD), de forma cogente, a metodologia de elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD), para as operações de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais dos titulares de dados pessoais.

Parágrafo único: Cada Unimed deve revisar seus relatórios de impacto anualmente, ou sempre que houver qualquer mudança no tratamento do dado pessoal, podendo, em qualquer tempo, ser solicitado pelo SEPD.

Art. 9º Deverão ser criados pelo SEPD, de forma cogente, planos de resposta a incidentes que envolvam dados pessoais, observado o parágrafo deste artigo.

Parágrafo único: Todos os alcançados por esta Norma devem atender a obrigação de comunicar formalmente ao Encarregado da Unimed Federação/RS, preenchendo no formulário de comunicação de incidente de segurança com dados pessoais, a suspeita ou a ocorrência de um incidente de segurança que possa resultar em um tratamento não autorizado de dados pessoais, bem como, atender às disposições legais neste sentido. Por sua vez, o Encarregado da Unimed Federação/RS, por atribuição legal, analisará o formulário e havendo a materialização do incidente, comunicará formalmente a Unidade onde ocorreu o incidente e avaliará a necessidade de comunicar o incidente à Autoridade Nacional e à Unimed do Brasil.

Todos os campos do formulário indicados como obrigatórios deverão ser preenchidos. O formulário deverá contemplar o incidente relacionado aos dados pessoais, com a apresentação de todas as informações disponíveis, incluindo a identificação de quais dados pessoais foram afetados e as medidas tomadas ou planejadas, para mitigar os efeitos de tal incidente.

CAPÍTULO III**EXTENSÃO E OBJETIVOS DO SISTEMA ESTADUAL DE PROTEÇÃO DE DADOS (SEPD)**

Art. 10 O SEPD abrange o conjunto das Cooperativas do Sistema Unimed do Estado do Rio Grande do Sul e entidades por elas constituídas.

Art. 11 O escopo do SEPD desdobra-se nos seguintes objetivos:

- I definição de métricas para avaliação de conformidades, mediante o estabelecimento de um Programa Permanente de Auditoria, cujo detalhamento está contido no ANEXO 1;
- II estabelecimento de diretrizes desse Programa, com foco na segurança e na proteção da privacidade;
- III fixação das regras de observação obrigatória na gestão de incidentes de vazamento de dados pessoais;
- IV orientação jurídica das condutas a serem observadas para a garantia da segurança das demais definições deste artigo; e
- V normatização de regras para atendimento dos objetivos previstos nos incisos deste artigo.

CAPÍTULO IV**COMPOSIÇÃO E COMPETÊNCIA DOS ÓRGÃOS DO SEPD**

Art. 12 O SEPD contará com uma Câmara Executiva e uma Câmara Deliberativa, assim constituídas:

- I A Câmara Executiva será coordenada pelo Encarregado da Unimed Federação/RS e integrada pelos técnicos por ele considerados indispensáveis ao desenvolvimento de suas tarefas;
- II A Câmara Deliberativa será constituída por:
 - a) um Diretor integrante da Diretoria Executiva da Unimed Federação/RS, pela mesma Diretoria indicado, que exercerá a função de Coordenador;
 - b) um Diretor integrante da Diretoria Executiva da Unimed Central de Serviços Auxiliares - RS, pela mesma Diretoria indicado;
 - c) um representante do Conselho de Administração (CA) da Unimed Federação/RS, que também é membro do CA da Unimed Central de Serviços Auxiliares - RS;
 - d) uma secretária executiva, que exercerá a função de organização das reuniões e confecção das atas; e
 - e) um representante da assessoria jurídica, que apoia a Câmara Executiva.

§ 1º Os integrantes possuem mandato de um ano, podendo, ao final deste período, serem reconduzidos automaticamente sem a necessidade de comunicação formal.

§ 2º O impedimento de um membro por período superior a três meses implicará na sua substituição, exercendo o substituto o mandato pelo prazo remanescente do substituído, também permitida a recondução.

§ 3º Reúnem-se uma vez por mês, com presença mínima de três de seus membros, dos quais um, necessariamente, será Diretor.

Art. 13 O Encarregado desenvolve as seguintes competências:

- I executa, com auxílio de equipe técnica, as atividades que são de sua competência institucional, fixadas na LGPD;

- II propõe normas e recomendações à Câmara Deliberativa; e
- III participa das reuniões da Câmara Deliberativa sempre que convocado.

Art. 14 A Câmara Deliberativa tem competência para as seguintes matérias:

- I apreciação de proposições do Encarregado para o estabelecimento de resoluções normativas e demais recomendações; e
- II recebimento de reclamações relacionadas ao SEPD, fornecendo respostas, ouvindo, necessariamente, o Encarregado.

Parágrafo único: A Câmara Deliberativa será assessorada, no que solicitar, pela equipe técnica que atua junto ao Encarregado.

CAPÍTULO V FORMAS DE COMUNICAÇÃO

Art. 15 O SEPD se expressa através dos seguintes documentos:

- I atas;
- II resoluções normativas;
- III manuais;
- IV informações;
- V orientações; e
- VI pareceres.

Parágrafo único: Os atos expedidos pela Unimed do Brasil sobre a matéria deverão ser observados, quando considerados cabíveis pelo SEPD, até a edição de ato interno que os suplante ou os complemente, observada adequação e conformidade dos mesmos na avaliação da equipe técnica estadual.

Art. 16 Atas são os documentos pelos quais a Câmara Deliberativa documenta suas deliberações, dentro de suas competências estatutárias e regimentais, devendo conter:

- I ordem do dia (conforme o caso);
- II assunto tratado, manifestações, transcritas em síntese, propostas e seus autores; e
- III suas deliberações, com ressalvas expressas, quando for o caso.

Art. 17 Resoluções normativas são normas administrativas propostas pela Câmara Executiva e aprovadas pela Câmara Deliberativa.

Art. 18 Manuais são instrumentos técnicos que visam elucidar tarefas administrativas, criados pela Câmara Executiva e aprovados pela Câmara Deliberativa.

CAPÍTULO VI SANÇÕES

Art. 19 As Cooperativas do Sistema Unimed do Estado do Rio Grande do Sul e as entidades por elas constituídas que não observarem as diretrizes dispostas na presente Norma serão responsabilizadas por todos os danos causados em decorrência da sua omissão, sem prejuízo de outras sanções previstas na legislação ou nas normas integrativas do Sistema Unimed.

Elas deverão obedecer a graus conforme a gravidade, reincidência, e incluir a necessidade de apresentação de plano de ação de correção da ocorrência.

CAPÍTULO VII DOCUMENTOS DA NORMA

Art. 20 Fazem parte desta Norma os seguintes documentos e anexos:

- I ANEXO I - METODOLOGIA DO PROGRAMA PERMANENTE DE AUDITORIA (PPA): documento que estabelece as regras e a metodologia para execução Programa Permanente de Auditoria (PPA), com foco na segurança da informação e proteção da privacidade;
- II ANEXO II - CRONOGRAMA DO CICLO DE EXECUÇÃO DO PLANO ANUAL DE AUDITORIA (PAA): estabelece as datas para o período de planejamento, divulgação do Caderno de Questões e Critérios, habilitação e pré-qualificação dos respondentes, coleta das informações auditáveis, análise e devolutiva do Relatório de Auditoria; e
- III ANEXO III - CADERNO DE QUESTÕES E CRITÉRIOS: sendo sua estrutura desenvolvida em dimensões que permitem o agrupamento de quesitos relativos a um determinado tema, além de ser dividido em questões de pré-qualificação e questões de auditoria.

Parágrafo único: Todos os anexos citados serão revisados periodicamente pelo SEPD.

CAPÍTULO VIII VIGÊNCIA E ALTERAÇÕES

Art. 21 Esta Norma entra em vigor na data de sua aprovação pelo Conselho de Administração, podendo, por este órgão, ser, a qualquer tempo, alterada e sendo por este, nos casos omissos, interpretada.

SÍNTESE DAS REVISÕES

Revisão	Data	Alterações	Aprovação
00	29/04/2022	- Documento de origem.	Conselho de Administração da Unimed Federação/RS