Sumário

1. OBJETIVO

Esta Política tem como objetivo apresentar as regras aplicáveis para o tratamento de dados pessoais realizados pela UNIMED FESP, tanto de pessoas relacionadas à sua estrutura interna, quanto de terceiros, em atenção às disposições da Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais ou "LGPD"), além de estabelecer os requisitos necessários para a construção de um programa de privacidade em conformidade com a referida legislação.

2. ÂMBITO DE APLICAÇÃO

Esta política aplica-se a todos os administradores (Diretores Estatutários, membros do Conselho de Administração, Conselho Fiscal, Comitês), colaboradores da Unimed Fesp, FespPart Participações S.A e empresas sócias e coligadas, bem como, por todos os seus respectivos administradores, colaboradores e prepostos a eles vinculados, considerando suas necessidades específicas e os aspectos legais e regulamentares a que estão sujeitas.

O cumprimento desta Política também é obrigatório a todos os Terceiros prestadores de serviços, e em especial quando:

a) A operação de tratamento tenha sido ou será realizada no território brasileiro;

b) A atividade de tratamento objetivar a oferta de bens ou serviços que envolva o tratamento de dados de indivíduos localizados dentro do território brasileiro; ou

c) Os dados pessoais objetos do tratamento tenham sido coletados dentro do território brasileiro.

3. DEFINIÇÕES

Anonimização: Processo por meio do qual o dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, considerados os meios técnicos razoáveis e disponíveis no momento do tratamento.

ANPD: Autoridade Nacional de Proteção de Dados.

Controlador: Pessoa a quem competem as decisões sobre o tratamento dos dados pessoais.

Dados Pessoais: Toda e qualquer informação relativa a uma pessoa natural identificada ou identificável.

Dados sensíveis: Dado pessoal que diga respeito a 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.

Encarregado ou DPO: a pessoa indicada para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) além das tarefas adicionais que lhe forem atribuídas pela FESP conforme permissivo previsto no artigo 41, §2º, IV e 41§3º da LGPD.

GRC: Sigla que significa Governança, Riscos e Compliance.

LGPD: Sigla de Lei Geral de Proteção de Dados. Lei Federal nº 13.709/2018, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Operador(a): Pessoa, física ou jurídica, que realiza o tratamento de dados pessoais em nome do(a) controlador(a).

Titular: Pessoa natural identificada ou identificável a quem se referem os dados pessoais.

Tratamento Irregular: O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - O modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Tratamento de dados: Toda operação efetuada com dados pessoais, por meios automatizados ou não, 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.

4. DIRETRIZES

4.1 Disposições Gerais

A UNIMED FESP tem o compromisso de tratar dados pessoais, sejam de seus colaboradores, seus clientes, fornecedores, parceiros e terceiros, com o mais alto nível de cuidado, confidencialidade e conformidade com as legislações aplicáveis. Seus colaboradores, gestores e administradores devem sempre, no exercício de suas atividades, garantir que dados pessoais sejam tratados em conformidade com a legislação aplicável e com esta Política e outros normativos internos que sejam aplicáveis.

Esta Política visa demonstrar o comprometimento da Unimed Fesp em:

a) Proteger os direitos dos colaboradores, clientes e parceiros;
b) Adotar processos e regras que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
c) Promover a transparência sobre a forma pela qual a Unimed Fesp trata dados pessoais;
d) Adotar medidas de proteção em relação a risco de incidente de segurança que envolva dados pessoais.

Para a UNIMED FESP, garantir o tratamento de dados pessoais de forma legítima e correta é fundamental para o sucesso de suas atividades, de forma a proteger a sua credibilidade perante colaboradores, clientes, fornecedores, parceiros, terceiros e ANPD.
Em caso de divergência entre o conteúdo desta Política e a legislação de proteção de dados aplicável, esta última prevalecerá.
Políticas adicionais poderão ser criadas para atender a casos específicos no que tange a privacidade e a proteção de dados, principalmente se exigido por lei ou regulamento.

4.2 Princípios norteadores da proteção de dados pessoais

As áreas responsáveis por fazer cumprir esta política, em conjunto com o Encarregado/DPO devem garantir para que todas atividades de tratamento de dados pessoais observem a boa-fé e estejam em conformidade com os princípios trazidos pela legislação sobre privacidade e proteção de dados. São eles:

a) Princípios da finalidade: o tratamento de dados pessoais deve atender a propósitos legítimos, específicos, explícitos e informados ao titular, sendo vedado o tratamento posterior de forma incompatível com essas finalidades.
b) Princípio da adequação: o tratamento de dados pessoais deve ser compatível com as finalidades informadas ao titular.
c) Princípio da necessidade: o tratamento de dados pessoais deverá ser limitado ao mínimo necessário para o cumprimento das finalidades pretendidas e expostas ao Titular, garantindo também que tais informações sejam armazenadas pelo menor tempo possível.
d) Princípio do livre acesso: aos titulares deverá ser garantida a consulta facilitada e gratuita quanto à forma e à duração do tratamento, bem como a integralidade de seus dados pessoais.
e) Princípio da qualidade dos dados: aos titulares deverá ser garantida a exatidão, a clareza, a relevância e a atualização dos dados pessoais.
f) Princípio da transparência: as informações sobre o tratamento e atuação do Controlador e/ou Operador devem ser claras, precisas e facilmente acessíveis, respeitados os segredos comercial e industrial.
g) Princípio da segurança: a Unimed Fesp deve adotar medidas técnicas e organizacionais aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
h) Princípio da prevenção: adoção de medidas técnicas e organizacionais a fim de prevenir a ocorrência de danos envolvendo dados pessoais.
i) Princípio da não discriminação: as atividades de tratamento de dados pessoais jamais poderão objetivar fins discriminatórios, ilícitos ou abusivos.
j) Princípio da responsabilização e prestação de contas: a Unimed Fesp deve armazenar os registros de todas as atividades de tratamento de dados pessoais e as respectivas medidas tomadas para adequar tais atividades às normas relativas à privacidade e proteção de dados, comprovando sua eficácia e eficiência.

4.3 Bases legais para o tratamento de dados pessoais

Para ser considerada legítima e adequada à LGPD, uma atividade de tratamento de dados pessoais realizada pelos responsáveis por fazer cumprir esta política, em conjunto com o Encarregado/DPO, deve estar apoiada em uma das hipóteses abaixo:

4.3.1 Cumprimento de obrigação legal

O tratamento de dados poderá ser realizado para o cumprimento de uma obrigação legal ou regulatória tal qual obrigações e licenças ambientais, controle de ponto de colaboradores, envio de dados ao E-Social, exames admissionais, arquivamento de notas fiscais.

É importante que o(s) responsável(is) pelo tratamento esteja ciente de qual a obrigação legal fundamenta o tratamento (lei, norma, regulação, decisão ou acordo judicial etc.). Caso haja alguma alteração nestas regras, é possível que a atividade de tratamento também deva ser alterada.

O Encarregado/DPO da UNIMED FESP deve ser consultado em caso de dúvidas quanto à necessidade de se tratar dados para o cumprimento de obrigações legais ou regulatórias.

4.3.2 Execução de contrato com o titular

Aplica-se quando se faz tratamento de **dados pessoais** fundamentada em um contrato firmado (ou prestes a ser firmado) com o titular, possibilitando que a Unimed Fesp cumpra com as obrigações estabelecidas neste documento.

4.3.3 Exercício regular de direitos

Para que o Encarregado garanta em nome da UNIMED FESP o(s) direito(s) de defesa, resposta, ou atuação junto a órgãos públicos, em processos judiciais ou administrativos, bem como nas hipóteses dispostas no §4º, do artigo 11 da LGPD, em especial para o compartilhamento de dados de saúde para finalidade comercial, pode-se manter guardados **dados pessoais** , ou documentos que contenham dados pessoais e dados pessoais sensíveis, sejam de colaboradores, dirigentes, clientes, fornecedores ou demais terceiros, visando garantir o direito de produção de provas, em observância aos preceitos constitucionais da ampla defesa e do contraditório.

A retenção dos dados não deve ultrapassar o período estabelecido na tabela de temporalidade documental, que, por sua vez, deve estar sempre atualizada com os prazos legais e prescricionais aplicáveis para estabelecimento do período de retenção.

4.3.4 Tutela da saúde

Dados pessoais e dados sensíveis são tratados para a realização de procedimentos e serviços de saúde. Nessa situação, sempre deve haver o envolvimento de um profissional de saúde, prestador de serviços de saúde ou autoridade sanitária.

4.3.5 Proteção à vida

Em caso de perigo ou iminência de perigo à sua vida ou incolumidade física, esta base legal pode ser utilizada para o tratamento de dados pessoais e dados pessoais sensíveis, prezando pela preservação da vida dos titulares (exemplo, protocolos de acidentes de trabalho e emergências médicas).

4.3.6 Proteção do crédito

Quando for permitida a avaliação de idoneidade financeira do titular dos **dados pessoais**, antes da comercialização de serviços e produtos.

4.3.7 Prevenção à fraude e segurança

A prevenção à fraude aplica-se a **dados sensíveis**, quando tratados em procedimentos de identificação e autenticação de cadastro em sistemas eletrônicos (exemplo: fechaduras / catracas biométricas, reconhecimento facial para segurança em cadastros). É primordial que o titular esteja ciente da utilização de seus dados para este fim, através de avisos complementares de privacidade.

4.3.8 Interesse legítimo do controlador / terceiros

O uso dessa base legal é uma excepcionalidade, somente pode ser utilizada para fundamentar interesses legítimos do controlador ou de terceiros, sendo que estes interesses não podem afetar de forma injusta ou desproporcional os direitos e liberdades dos titulares. Alguns exemplos: estudos e relatórios internos sobre as atividades da Unimed

Fesp; avaliações de desempenho de colaboradores; oferta de serviços adicionais a titulares que já são clientes.

As atividades baseadas nesta hipótese não devem conter dados pessoais sensíveis (vide conceito no item 3 desta Política). Além disto, devem somente envolver **dados pessoais de titulares que já possuem alguma relação com a UNIMED FESP**, sejam clientes, ex-clientes, colaboradores etc. Devem, essencialmente, ocorrer dentro das legítimas expectativas do titular dos dados, de forma que ele deve razoavelmente esperar que seus dados sejam tratados para as respectivas finalidades baseadas no interesse legítimo da UNIMED FESP.

O Encarregado tem a responsabilidade de revisar e avaliar todas as atividades de que envolvam tratamento de dados pessoais, sobretudo as realizadas com base no interesse legítimo, o que deve ser feito, preferencialmente desde a concepção de novos produtos e projetos. Nessa avaliação, deve ser elaborado o **Relatório de Impacto à Proteção de Dados,** conforme item 4.11, com o apoio do responsável pela atividade.

4.3.9 Consentimento do titular

Em caráter de excepcionalidade, algumas áreas coletam o consentimento do titular dos dados, o qual concede autorização mediante manifestação livre, espontânea, inequívoca e para finalidades determinadas. Esta base legal poderá ser utilizada para justificar o tratamento de dados pessoais e dados sensíveis, quando as atividades não se enquadram nas demais hipóteses, ou, eventualmente, quando houver determinação regulatória para a coleta de consentimento do beneficiário.

Além disto, a UNIMED FESP deverá implementar mecanismo de fácil revogação do consentimento coletado, bem como a verificação das atividades baseadas no consentimento, para avaliar se há aderência entre a finalidade atual da operação e o consentimento colhido.

4.3.10 Outras bases legais

Algumas áreas podem tratar dados pessoais e dados pessoais sensíveis com base nas demais hipóteses trazidas pela LGPD, desde que os possíveis riscos sejam avaliados com

o Encarregado ou Núcleo de Privacidade, de acordo com a criticidade dos dados envolvidos.

Para auxiliar, segue abaixo quadro orientativo sobre as bases legais para tratamento de dados:

Hipóteses de Tratamentos dos Dados Pessoais, art. 7º, LGPD	**Hipóteses tratamentos dos Dados Pessoais Sensíveis, art. 11º, LGPD**
I – Consentimento pelo titular de forma específica e destacada, para finalidades específicas.	I – Consentimento pelo titular de forma específica e destacada, para finalidades específicas;
II – Para o cumprimento de obrigação legal ou regulatória pelo controlador;	II, “a” - para o cumprimento de obrigação legal ou regulatória pelo controlador;
V – Execução de contrato ou de procedimentos preliminares relacionados a contrato;	Não há essa hipótese;
VI – Para o exercício regular de direitos em processo judicial, administrativo ou arbitral;	II, “d” - exercício regular de direitos, em contrato e em processo judicial, administrativo e arbitral;
VII – para a proteção da vida ou da incolumidade física do titular ou de terceiros;	II, “e” – proteção da vida ou da incolumidade física do titular ou de terceiros;
VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;	II, “e” - tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
IX – Legítimo interesse;	Não há essa hipótese;

X – Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente;	Não há essa hipótese;
Não há essa hipótese de forma expressa, embora o entendimento seja que já esteja incorporada na hipótese do legítimo interesse, art. 7º, inciso IX.	II, “g” garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

4.4 Governança de Dados e Programa de Privacidade

Para que o programa de privacidade da UNIMED FESP se mostre efetivo e produza resultados positivos, é importante que os pilares e procedimentos da Unimed Fesp sejam constantemente observados durante as operações de tratamento de dados pessoais.

4.4.1 Políticas, Procedimentos e Documentos do Programa de Privacidade

É fundamental que todos os colaboradores, gestores, diretores, colaboradores, prestadores de serviços, dentre outros, observem as políticas e procedimentos que compõem o Programa de Privacidade da UNIMED FESP. Além disso, é importante que esta observância e o cumprimento de todas obrigações da lei sejam bem definidos, documentados e registrados.

A área de GRC da UNIMED FESP, em conjunto com os responsáveis por cada um dos temas abaixo, instituiu os documentos elencados abaixo na sua estrutura de governança de dados:

a) Política de Segurança da Informação;
b) Termo de Responsabilidade e Confidencialidade;
c) Norma de Resposta a Incidentes de Violação de Dados Pessoais;
d) Aviso Interno de Privacidade e Proteção de Dados;
e) Norma para coleta de consentimento;
f) Aviso Geral de Privacidade e Proteção de Dados
g) Relatório de Impacto à Proteção de Dados Pessoais
h) Notificação de Incidente de Segurança

4.4.2 Responsáveis pelo Programa de Privacidade

Para facilitar o controle de conteúdo, datas de publicação e prazos para revisão, os documentos de governança relacionados à privacidade (incluindo esta política) devem ser controlados e gerenciados de forma centralizada pelos responsáveis abaixo:

4.4.2.1 Núcleo de privacidade

O Núcleo de privacidade deve ser composto por integrantes de áreas-chave da UNIMED FESP, capazes de deliberar e decidir sobre assuntos relacionados à privacidade e proteção de dados, incluindo representantes dos departamentos Jurídico, GRC, Segurança da Informação e Gestão de Pessoas. Adicionalmente, podem ser chamados, para deliberação de assuntos específicos, representantes de áreas envolvidas em atividades de tratamento de dados pessoais.

Entre as atividades do Núcleo de privacidade estão a garantia da comunicação do programa de privacidade, discussão e tomada de decisões sobre atividades de tratamento que envolvem riscos classificados como altos, levantados através de Relatórios de Impacto à Proteção de Dados Pessoais. Caso o risco seja considerado muito alto, a decisão deverá ser escalada junto à Alta Administração.

4.4.2.2 Encarregado de Proteção de Dados / DPO

O Encarregado de Proteção de Dados tem como missão garantir a conformidade da UNIMED FESP em relação às leis e demais normas de privacidade e proteção de dados aplicáveis, através do Programa de Privacidade.

Entre as funções determinadas para o Encarregado estão:

a) Gestão do programa de privacidade;
b) Desenvolvimento, manutenção e revisão das normas e políticas de privacidade da Unimed Fesp, inclusive desta política;
c) Fiscalização do cumprimento das normas e políticas de privacidade da Unimed Fesp;
d) Monitoramento do nível de conformidade da Unimed Fesp, através de análises de diagnóstico periódicas, com a definição de planos de ação para disseminação das políticas de privacidade;

e) Ponto focal para autoridade nacional de proteção de dados e os titulares dos dados;
f) Recepção e resposta as eventuais requisições realizadas por titulares de dados pessoais;
g) Confecção dos Relatórios de Impacto à Proteção de Dados Pessoais, com apuração e revisão dos riscos das atividades nele relatadas.

É de responsabilidade do Encarregado a decisão, em casos de risco baixo a moderado, sobre as atividades de tratamento de dados pessoais conduzidas pela UNIMED FESP. Caso o risco seja considerado alto, a decisão deverá ser escalada ao Núcleo de privacidade.

Compete também ao Encarregado auxiliar os colaboradores da UNIMED FESP e orientar-lhes sobre dúvidas quanto ao Programa de Privacidade e a forma correta de tratamento de Dados Pessoais a ser adotada durante a execução de suas atividades.

4.5 Registro de Operações de Tratamento de Dados Pessoais

O Encarregado é responsável pela manutenção do registro de operações de tratamento de dados pessoais, podendo contar com a ajuda dos gerentes das áreas.

O Encarregado deve garantir que os responsáveis pelo tratamento de dados mantenham o registro de todas as suas operações de tratamento destes, contendo, no mínimo, as seguintes informações sobre cada operação:

a) Descrição do fluxo da informação em cada etapa de seu ciclo de vida (coleta, armazenamento, uso, compartilhamento – e neste caso, a finalidade para transferência – e descarte);
b) Base legal para tratamento;
c) Tipos de dados pessoais coletados;
d) Finalidade para o qual o dado é tratado;
e) Local lógico (nuvem, servidor, laptop etc.) e geográfico onde o dado é tratado;
f) Período de retenção do dado;
g) Área responsável pelo dado;
h) Volume aproximado de registros existentes.

4.6 Treinamentos

Colaboradores da UNIMED FESP que estejam envolvidos nas atividades de tratamento de dados pessoais deverão receber treinamentos periódicos, decididos pelo Núcleo de Privacidade e organizado pelo Encarregado, especificamente sobre:

a) Conceitos gerais de Privacidade e Proteção de Dados, incluindo a apresentação desta política e de materiais de estudo sobre os princípios da LGPD;
b) Conceitos específicos de Privacidade e Proteção de Dados, aplicados às atividades de cada área.

4.7 Transparência

As operações envolvendo atividades de tratamento de dados pessoais de titulares externos (terceiros/parceiros/clientes), deverão observar o Aviso Geral de Privacidade e Proteção de Dados.

Todas as operações envolvendo atividades de tratamento de dados pessoais de titulares internos (colaboradores), deverão observar o Aviso Interno de Privacidade e Proteção de Dados.

Se qualquer área da UNIMED FESP promova atividade que envolva o tratamento de dados pessoais de formas que, excepcionalmente, não se enquadrem no respectivo Aviso de Privacidade, não contendo neste informações claras e suficientes sobre os pontos elencados abaixo, será imprescindível a apresentação de aviso específico para complementação das informações fornecidas ao titular, devendo ser validado pelo Encarregado e disponibilizado antes que os dados pessoais sejam efetivamente tratados:

a) Escopo da atividade;
b) Quais os dados envolvidos na atividade;
c) Finalidade da atividade de tratamento;
d) Forma e duração do tratamento;
e) Descrição da forma de coleta, utilização, armazenagem e descarte das informações;
f) Informações sobre os agentes de tratamento envolvidos na atividade;
g) A eventual existência de decisões automatizadas incorporadas na atividade.

4.8 Consentimento

O Encarregado deverá avaliar e validar quanto à exigência de consentimento para a atividade e a impossibilidade de seu enquadramento em outras bases legais, bem como revisar a forma de coleta do consentimento, que deverá observar os pontos a seguir:

a) Manifestação livre: O titular deve fornecer o consentimento de maneira livre, sem que seja forçado a dar o consentimento para que possa usufruir do serviço/produto relacionado;
b) Manifestação granular: O titular forneceu a sua autorização (consentimento) para que fosse realizado o tratamento em situações específicas e determinadas (Exemplo: “Aceito que meus dados pessoais sejam utilizados para fins estatísticos, para melhorias da plataforma de serviços”);
c) Manifestação informada: O titular, teve acesso ao Aviso de Privacidade correspondente a atividade na qual foi sujeitado, antes do fornecimento de sua autorização, garantindo possuir plena ciência da finalidade e dos limites da atividade de tratamento realizada;
d) Manifestação inequívoca: O titular forneceu os seus dados pessoais, sem qualquer dúvida ou questionamento quanto aos limites da atividade.

As áreas responsáveis por coletar os termos de consentimento, por exemplo, Gestão de Pessoas, Contas Médicas, Tecnologia da Informação, dentre outras, devem ter evidências de documentação, armazenamento e gestão da autorização concedida para assegurar que o consentimento foi coletado de maneira correta, possibilitando a demonstração dessa atividade tanto ao próprio titular como para a Autoridade Nacional de Dados Pessoais - ANPD, bem como para garantir ao titular o direito à revogação do consentimento.

4.9 Segurança da Informação

Os responsáveis pelos procedimentos e ferramentas de Segurança da Informação devem manter seu controle interno a fim de evitar a ocorrência de acessos indevidos ou não autorizados, perda, destruição ou qualquer outra ação que comprometa a integridade, disponibilidade ou confidencialidade dados pessoais tratados no decorrer de suas atividades.

Em casos de ocorrência de incidentes envolvendo dados pessoais, o Encarregado deve demonstrar procedimento para mitigação das consequências, que está disponível e pode ser consultado no Procedimento de Resposta a Incidentes de Violação de Dados Pessoais e manter contato de forma rotineira com o(s) responsável(is) por esses registros garantindo assim seu devido controle**.**

O Encarregado de Dados deve manter em conjunto com a(s) área(s) responsável(is) um canal público para recebimento de notícias de incidentes, que pode ser utilizado por público externo e interno. Comunicações devem ser recebidas pelo Encarregado, que verificará o ocorrido e procederá à aplicação do procedimento acima citado.

4.10 Coleta, uso, armazenamento e descarte de dados

As atividades de tratamento de dados pessoais realizadas pela(s) área(s) que assim o fazem e, devidamente mapeadas, devem ocorrer em respeito a todos os pilares deste documento, apoiadas em base legal específica, conforme item 4.3 (Bases legais para o tratamento de dados pessoais).

4.10.1 Coleta de Dados Pessoais

A atividade de coleta de dados pessoais deve ser limitada àqueles necessários para o cumprimento da finalidade determinada e informada ao titular dos dados. Deve-se ressaltar a necessidade de manter os dados coletados sempre atualizados.

Os titulares dos dados pessoais devem ser informados, antes da coleta de dados realizada em pontos ativos (ou seja, onde os titulares fornecem seus próprios dados), de todos os detalhes sobre a atividade de tratamento, conforme o item 4.7.

A coleta de dados pessoais em pontos passivos (pelo acesso a bases públicas/privadas de dados) somente poderá ocorrer se essas bases forem notoriamente fidedignas (atribuídas a órgãos ou entidades públicas e oficiais), se houver contrato entre o provedor da base e a UNIMED FESP, ou mediante expressa autorização do Encarregado ou do Núcleo de Privacidade.

Para que terceiros possam compartilhar dados pessoais com a UNIMED FESP é fundamental que no contrato celebrado entre as partes exista cláusula de privacidade capaz de garantir a integridade e a confiabilidade das informações compartilhadas, além do

compromisso com normas específicas relativas à privacidade e proteção de dados pessoais. A idoneidade desses terceiros também deve ser verificada pelos responsáveis por tal ação.

Os dados pessoais informados pelos terceiros devem possuir descrição completa do seu ciclo de vida, antes do compartilhamento com a(s) área(s) que realizam tratamento de dados na UNIMED FESP, demonstrando que, em nenhuma destas etapas, tenha ocorrido qualquer forma de tratamento ilícito ou inadequado.

4.10.2 Uso de Dados Pessoais

O uso de dados pessoais deve sempre atender à expectativa gerada ao titular dos dados quando este fora informado da finalidade da coleta das informações, mesmo em casos de coleta realizada por terceiros. Se houver alteração da finalidade previamente informada ao titular, este deve ser novamente informado sobre as intenções da(s) área(s) responsável(is) da UNIMED FESP, avaliando a necessidade de qualquer adequação.

O dado não deve ser utilizado para outra finalidade, exceto com a ciência / expectativa do titular e, devidamente documentação/formalizada.

4.10.3 Armazenamento de Dados Pessoais

Dados pessoais devem ser armazenados pelo tempo mínimo indispensável para atendimento da finalidade pretendida e cumprimento de eventuais obrigações legais que regulam a atividade de tratamento. Após o cumprimento da finalidade e término de prazos legais de retenção, os dados deverão ser descartados, o que por sua vez deverá seguir meios adequados, conforme abaixo:

a) Documentos e dados em formato físico: O descarte deve ser realizado por meio de trituradores de papel, sendo proibido o uso direto de lixeiras.

b) Documentos e dados em formato eletrônico: o descarte deve ocorrer conforme definido em documento específico da área de Segurança da informação, garantindo

inclusive sua destruição nos servidores, fitas backup e quaisquer outros tipos de repositório de dados tecnológicos, desde que não seja justificada sua guarda.

Para fins estatísticos e de pesquisa, alguns dados pessoais podem passar por procedimento de anonimização permanente, validado pelo Encarregado e devidamente formalizado.

4.10.4 Tratamento de dados pessoais sensíveis e dados de crianças e adolescentes

A Lei Geral de Proteção de Dados classifica alguns dados como sensíveis, devido a capacidade de gerar discriminação ao titular destas informações. Alguns exemplos de dados pessoais sensíveis são a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a Organização de carácter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando relacionados a um indivíduo.

Os dados pessoais sensíveis que são tratados pela UNIMED FESP em suas operações são considerados lícitos e legítimos, baseando-se nas bases legais previstas pela LGPD, conforme item 4.3, e recebem a máxima prioridade na Segurança de Informação.

O tratamento de dados pessoais de “crianças” e “adolescentes” deve ser realizado:

a) Voltado ao melhor interesse de tais indivíduos, ou seja, com a finalidade de beneficiá-los, ainda que de forma indireta;
b) De modo que informações destinadas a este público sejam prestadas de modo claro, acessível, consideradas as condições físico-motoras, perceptivas, sensoriais, intelectuais e mentais dos destinatários, com o uso de recursos audiovisuais, quando adequado.

Sobre tratamento dos dados de crianças e adolescentes menores de idade, deve haver a coleta do consentimento específico dado por pelo menos um dos pais ou pelo responsável legal, mantendo públicas as informações sobre o tipo de dados coletados, a forma de utilização e as garantias dos demais direitos dos titulares assegurados pela lei.

4.11 Relatório de impacto à proteção de dados pessoais

Os relatórios de impacto à proteção de dados pessoais são documentos que possuem a descrição dos processos que envolvem o tratamento de dados pessoais que, por sua natureza, são passíveis de gerar riscos às liberdades civis e individuais dos titulares dos dados pessoais. Este documento deve ser elaborado quando:

a) Da realização de operações de tratamento de dados pessoais sensíveis;
b) Da realização e condução de operações que envolvam o tratamento de dados críticos, passíveis de gerar altos riscos aos titulares de dados pessoais em caso de ocorrência de incidentes envolvendo tais informações;
c) A operação de tratamento de dados pessoais estiver amparada na base legal do interesse legítimo.

Quando houver necessidade de elaboração deste documento, o gestor da área responsável pela atividade de tratamento dos dados deve ser o responsável pela elaboração, submetendo posteriormente o documento para avaliação do Encarregado, que fará um parecer final sobre a atividade de tratamento.

4.12 Direitos dos titulares

A UNIMED FESP deve buscar garantir em todas as atividades de tratamento de dados pessoais os direitos dos titulares. A identidade dos titulares requerentes deve ser verificada e o atendimento deve acontecer sob a orientação do Encarregado.

Para recebimento de requisições de exercício dos direitos dos titulares, a UNIMED FESP possui canais abertos e direcionados, conforme abaixo:

Para colaboradores	Para clientes, parceiros ou terceiros
http://www.unimedfesp.coop.br/fale-conosco	http://www.unimedfesp.coop.br/fale-conosco

Eventual decisão de recusa, parcial ou total, no atendimento às requisições de titulares deve ser validada pelo Encarregado.

4.12.1 Direito à Informação e ao Acesso

É garantido o direito de confirmação da existência de tratamento de dados pessoais ao titular, mediante sua expressa requisição. A área de Governança de TI deve utilizar meios eficazes, cuja gestão e sua operacionalização deve ser supervisionada pelo Encarregado, mediante requisição do titular, por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa.

Quando em formato simplificado, o conjunto de dados deve ser entregue de imediato ao Encarregado.

Quando solicitado de forma completa, deve ser fornecido no prazo de até 15 (quinze) dias, contado da data do requerimento do titular e com as informações abaixo:

a) Inexistência de registro;
b) Origem dos dados;
c) Critérios utilizados;
d) Finalidade do tratamento.

Quando o tratamento tiver como origem o consentimento do titular ou contrato celebrado com o titular, este poderá solicitar cópia eletrônica integral de seus dados pessoais em formato que permita a sua utilização subsequente, até mesmo em outras operações de tratamento.

4.12.2 Direito a Retificação

É dado ao titular dos dados o direito de obter, a qualquer momento e mediante requisição, a correção de seus dados pessoais, quando incompletos, inexatos ou desatualizados.

4.12.3 Direito à exclusão, anonimização e bloqueio dos dados pessoais

O titular também pode requerer, a qualquer momento e mediante requisição, a eliminação, a anonimização ou o bloqueio de seus dados pessoais, quando as informações se mostrarem excessivas ou o tratamento dado pelo controlador estiver em desacordo com as determinações da LGPD.

Quando o titular solicitar a eliminação de dados pessoais, o Encarregado deve verificar se o tratamento dos dados objeto de requisição se justifica em algumas das bases legais listadas abaixo. Nesse caso, o direito do titular dos dados não deverá prevalecer:

a) Cumprimento de obrigação legal ou regulatória;

b) Estudo por órgão de pesquisa;
c) Transferência a terceiro, desde que respeitados os requisitos de Tratamento de dados dispostos em lei;
d) Uso exclusivo do controlador, vedado seu acesso por terceiros, e desde que os dados sejam mantidos anonimizados.

4.12.4 Direito à Oposição

O titular dos dados pode se opor, a qualquer momento e mediante requisição, ao tratamento de seus dados pessoais, quando a base legal do tratamento não for o consentimento. Este direito só será garantido e exercível quando for comprovado que a UNIMED FESP tratou dados pessoais de forma irregular, conforme artigos 18, §2º, c/c 44 da LGPD, devendo ser avaliado pela área Jurídica e, quando for o caso, por escritório independente a fim de mitigar o risco de conflito de interesse.

4.12.5 Direito à portabilidade

É garantido ao titular dos dados o direito de, a qualquer momento e mediante requisição, solicitar a portabilidade dos seus dados pessoais a outro fornecedor de serviço ou produto. Para atendimento a essa solicitação do titular é necessário que os dados pessoais do titular requerente sejam desvinculados de dados de outros titulares, e fornecidos em formato Interoperável, tal como.xls, .xlsx, .csv ou JSON.

4.12.6 Direitos atrelados ao consentimento

Mediante requisição e a qualquer momento, o titular pode solicitar informação sobre a possibilidade de não fornecer consentimento e as consequências de sua negativa, bem como de sua revogação.

4.12.7 Informação sobre compartilhamento de dados

A UNIMED FESP deverá garantir, por meio dos devidos controles, com quais entidades, públicas ou privadas, foram compartilhados dados pessoais, para que seja informado ao titular quando assim, expressamente, for solicitado.

4.13 Compartilhamento de dados pessoais com terceiros

Em situações onde seja necessária a transferência ou o compartilhamento de dados pessoais para terceiros (considerados “operadores”), para a prestação de um serviço específico ou atendimento de uma demanda pontual, o Encarregado de Dados deve, em conjunto com seus parceiros da área Jurídica, formalizar instrumentos contratuais que sejam capazes de garantir a integridade e a confiabilidade das informações compartilhadas, e também respeito às normas específicas relativas à privacidade e proteção de dados pessoais.

4.14 Transferência internacional de dados pessoais

Em situações onde seja necessária a transferência de dados pessoais para países estrangeiros, a área de Governança de TI juntamente com o Encarregado deve adotar uma das medidas abaixo, primordiais para garantir a integridade, a disponibilidade e a confidencialidade dos dados pessoais, conforme regulamentação da ANPD:

a) Avaliar se os dados pessoais serão transferidos para países com níveis de proteção de dados pessoais considerado como adequado pela ANPD.
b) Fornecer salvaguardas adequadas, no formato de: (a) cláusulas contratuais específicas para determinada transferência; (b) cláusulas-padrão contratuais; (c) normas corporativas globais; e (d) selos, certificados e códigos de conduta regularmente emitidos.
c) Coletar o consentimento específico do titular de dados pessoais;
d) Verificar a exigência por Lei para a tutela da saúde e demais circunstâncias específicas;
e) Quando expressamente autorizado pela Autoridade Nacional de Dados Pessoais.

4.15 Cookies

Cookies são arquivos ou informações que podem ser armazenadas em seus dispositivos quando você visita o site ou utiliza os serviços on-line da Unimed FESP.

4.15.1 Tipos de cookies

- **Necessários:** Os cookies são essenciais para que os websites da UNIMED FESP carreguem adequadamente e permitam que você navegue corretamente.
- **Desempenho:** Os cookies nos ajudam a entender como os visitantes interagem com as páginas da UNIMED FESP, fornecendo informações sobre as áreas visitadas, o tempo de visita ao site e quaisquer problemas encontrados, como mensagens de erro.
- **Funcionais:** Os cookies permitem que as páginas da UNIMED FESP se lembrem de suas escolhas, para proporcionar uma experiência personalizada.
- **Marketing:** Os cookies são utilizados para fornecer mais conteúdo relevante a você. Podem ser utilizados para apresentar publicidade e permitem a medição da eficácia de uma campanha publicitária lançada.

5. RESPONSABILIDADES

Para que esta Política atinja os efeitos pretendidos, é fundamental que todos os colaboradores, gestores, diretores, prestadores de serviços, dentre outros, atuem de acordo com os princípios definidos pela LGPD e cumpram as diretrizes de privacidade e proteção de dados pessoais, atentando-se ao fato de que os atos de quaisquer colaboradores da UNIMED FESP podem repercutir para o sistema como um todo, produzindo efeitos imprevisíveis.

O Encarregado de Proteção de Dados estará à disposição para atendimento a todos os colaboradores da UNIMED FESP.

A. Conselho de Administração/ Diretoria Executiva

- Fazer cumprir as regras constantes nesta política.

B. Gestores/ Líderes de Áreas

- Assegurar que os colaboradores estejam conscientes da importância da prática da boa segurança nas atividades diárias, e solicitar/providenciar educação e treinamento adequados e apropriados às suas responsabilidades, incluindo aspectos relevantes da legislação, regulamentos, direitos autorais e contratos;
- Acompanhar o cumprimento dessa política.

- Comunicar à área de Governança Corporativa os casos de descumprimento de Políticas, Normas ou Procedimentos internos, e os casos de falhas na execução de atividades operacionais.

C. Governança de TI

- Revisar as regras de proteção estabelecidas visando verificar: vazamento de informações; acessos inadequados, repasse de conteúdo inadequado, tentativa de quebra de controles de segurança da informação e armazenamento de arquivos multimídia que não façam parte do negócio da UNIMED FESP;
- Compreender os mecanismos de segurança a serem implementados a fim de prevenir, detectar ou corrigir incidentes envolvendo dados pessoais para evitar vazamentos ou acessos indevidos.

D. Gestão de Pessoas

- Comprometer-se a ter evidências de documentação, armazenamento e gestão da autorização concedida para assegurar que o consentimento foi coletado de maneira correta;
- Comprometer-se com o suporte estratégico no desenvolvimento de ações de divulgação desta política;
- Divulgar no processo de integração (treinamento) para todos os usuários (colaboradores, prestadores de serviços e terceiros) as principais diretrizes definidas por esta política.

E. Jurídico

- Obrigatoriedade de prestação de contas comprovando o tratamento dos dados pessoais e que esta Política está sendo integralmente cumprida, sendo que uma das formas de atendimento é através do Relatório de Impacto de Proteção de Dados;
- Respaldo Jurídico na necessidade da avaliação, análise e aplicação dos requisitos normativos nos processos de tratamentos de dados realizado pela Unimed Fesp.

F. GRC

A estrutura de Governança Corporativa visa garantir integridade, transparência, mitigação de riscos e credibilidade da marca, em conformidade com as melhores práticas do mercado e no âmbito dos órgãos reguladores e fiscalizadores, contribuindo para a sustentabilidade da UNIMED FESP. São atribuições das áreas sob sua estrutura, envolvidas na Governança de Dados e Programa de Privacidade:

- **Gestão da Qualidade & Controles Internos:** realizam a gestão de documentos controlados, mapeamento dos processos e avaliação de controles internos, garantindo que estes sejam efetivos e consistentes com a natureza, complexidade e riscos das operações. Avalia e desenvolve em conjunto as áreas Fluxo de Processos, Normas, Manuais, Procedimentos e Formulários.
- **Compliance:** garantem a conformidade da UNIMED FESP com legislações, regulamentações, políticas, normas e procedimentos, externos e internos, e com os princípios corporativos que garantem as melhores práticas de mercado e de Governança Corporativa. Contam com o apoio dos Agentes de Compliance, facilitadores nas áreas da UNIMED FESP para implementação e divulgação desta Política.
- **Gestão de Riscos & Prevenção à Fraude:** estabelece um conjunto de princípios, diretrizes, papéis e responsabilidades relacionados às práticas de Gestão de Riscos adotadas pela UNIMED FESP.
- **Secretaria de Governança:** Contribui para que as reuniões ocorram de modo consistente e em sincronismo com o exigido pelo Planejamento Estratégico, para que os registros das deliberações sejam disseminados e concretizados pelos agentes de governança. As reuniões estatutárias (CA, DE, CP, FI e CF), bem como reuniões executivas são acompanhadas pela Secretaria de Governança

Ainda sob a mesma gestão, porém de forma independente e segregada da estrutura de GRC temos:

- **Auditoria Interna:** afere, de forma independente, as regras e os procedimentos estabelecidos nesta Política, identificando, avaliando e mitigando os riscos, conferindo a aplicabilidade de procedimentos e rotinas além de disseminar a cultura de melhoria contínua dos processos

6. GESTÃO DE CONSEQUÊNCIA

Colaboradores, fornecedores ou outros *stakeholders* que observarem quaisquer desvios às diretrizes desta Política, poderão relatar o fato ao Canal de Ética (https://www.contatoseguro.com.br/unimedfesp), podendo ou não se identificar.

O descumprimento das diretrizes desta Política acarretará aplicação de medidas cabíveis conforme o respectivo grau de importância e de acordo com normativos internos.

Situações excepcionais serão encaminhadas para a Diretoria Executiva e/ou demais órgãos de Governança.

7. REFERÊNCIAS

Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais, “LGPD”

Norma Derivada nº 015/19 - Sobre a Política Nacional de Proteção de Dados Pessoais do Sistema Unimed.

8. DOCUMENTAÇÃO COMPLEMENTAR

Código de Conduta

Termo de Responsabilidade e Confidencialidade

PL 1444-01 Anticorrupção

PL 1447-01 Compliance

PL 1445-01 Gestão de Riscos

PL 1044-01 Política de Utilização de Recursos de TI

PL 1443-01 Política de Segurança da Informação

NO 1453-01 Resposta a Incidentes de Violação de Dados Pessoais

FQ 1453-04 Aviso Interno de Privacidade e Proteção de Dados

FQ 1453-05 Aviso Geral de Privacidade e Proteção de Dados

FQ 1453-03 Relatório de Impacto à Proteção de Dados

Pessoais FQ 1453-01 Comunicação de Incidentes ANPD

FQ 1453-02 Comunicação de Incidentes Titular

9. DISPOSIÇÕES GERAIS

É competência do Encarregado de Dados da UNIMED FESP alterar esta Política, sempre que necessário.

Esta Política entra em vigor na data de sua aprovação pela Diretoria Executiva e revoga quaisquer normas e procedimentos em contrário.