Política Geral de Proteção de Dados Pessoais

I. INTRODUÇÃO

Esta Política tem o propósito de estabelecer as diretrizes gerais para a proteção dos dados pessoais tratados pela Rede de Saúde da Divina Providência (RSDP), servindo de apoio para todas as práticas e processos internos relativos ao tratamento de dados pessoais, que deverão ser pautados sempre de acordo com os termos aqui dispostos e com as previsões disciplinadas nas demais normas internas aplicáveis, a fim de atender os objetivos abaixo descritos.

II. OBJETIVOS

- Tratar a privacidade, a proteção de dados pessoais e a autodeterminação informativa como direitos fundamentais da pessoa natural, garantidos pela Constituição Federal/88.
- Garantir a conformidade com as leis aplicáveis à proteção de dados pessoais, especialmente à LGPD – Lei Geral de Proteção de Dados Pessoais, Lei n° 13.709/2018.
- Orientar os envolvidos nas melhores práticas para o tratamento de dados pessoais.
- Atender aos direitos dos titulares de dados pessoais e protegê-los de eventuais incidentes.

III. DEFINIÇÕES

- Controlador: Agente de tratamento, pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
- Dado pessoal: Qualquer informação relacionada a uma pessoa física identificada ou identificável.
- Dado pessoal sensível: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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;
- Encarregado de Proteção de Dados Pessoais/*Data Protection Officer* (DPO): Pessoa indicada pelo controlador e operador, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados Pessoais.
- Incidente: Evento ou circunstância que poderia ter resultado, ou resultou, em dano desnecessário ao paciente. Os incidentes surgem quer de atos intencionais, quer de atos não intencionais.

- Risco: Probabilidade de um incidente ocorrer.
- Operador: Agente de tratamento, pessoa natural ou jurídica, de direito público ou privado, que realiza
o tratamento de dados pessoais em nome do controlador.
- Pessoas Colaboradoras: Pessoas contratadas pela RSDP de todos os níveis hierárquicos, residentes, estudantes, estagiárias, aprendizes, integrantes do corpo clínico e terceiras.
- Política de proteção de dados pessoais: Documento que estabelece as diretrizes gerais para a proteção dos dados pessoais tratados pela organização.
- Titular: Pessoa natural (física) a quem se referem os dados pessoais que são objetos do tratamento.
- Tratamento de dados pessoais: Toda a operação realizada com os dados pessoais, como a coleta, o armazenamento e o compartilhamento de dados pessoais.

IV. SIGLAS

- ANPD: Autoridade Nacional de Proteção de Dados.
- ANS: Agência Nacional de Saúde Suplementar.
- CFM: Conselho Federal de Medicina.
- CFF: Conselho Federal de Farmácia.
- CNSaúde: Confederação Nacional de Saúde.
- COFEN: Conselho Federal de Enfermagem.
- LGPD: Lei Geral de Proteção de Dados Pessoais.
- NR: Normas Regulamentadoras.
- RSDP: Rede de Saúde da Divina Providência.

V. DESCRIÇÃO

1. Abrangência

Esta Política é aplicável a todas as pessoas que integram a RSDP, tais como religiosas, diretores, lideranças, profissionais da saúde e demais pessoas colaboradoras, devendo ser cumprida por todas as pessoas envolvidas com o tratamento de dados pessoais, tanto em meios físicos, quanto digitais, independentemente do meio ou do país onde estejam localizados os dados, desde que tenham sido coletados em território nacional. As diretrizes estabelecidas nesta Política deverão ser aplicadas, seguindo os princípios reconhecidos pela Lei Geral de Proteção de Dados Pessoais (LGPD).

2. Princípios

A RSDP cumprirá, criteriosamente, os requisitos constantes na LGPD, de forma que os princípios abrangidos nesta Política sejam levados em conta: (a) na implementação de todos os procedimentos que impliquem o tratamento de dados pessoais, (b) nos produtos e/ou serviços oferecidos, (c) em todos os contratos celebrados com os

operadores de dados pessoais e (d) na implantação dos sistemas e plataformas, que permitam o acesso pelas pessoas colaboradoras ou por terceiros aos dados pessoais e/ou o tratamento desses dados.

As atividades de tratamento de dados pessoais deverão observar a boa-fé e demais princípios, conforme disposto no artigo 6º da LGPD:

(i) finalidade: *realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;*
(ii) adequação: *compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;*
(iii) necessidade: *limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;*
(iv) livre acesso: *garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;*
(v) qualidade dos dados: *garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;*
(vi) transparência: *garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;*
(vii) segurança: *utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;*
(viii) prevenção: *adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;*
(ix) não-discriminação: *impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;*
(x) responsabilização e prestação de contas: *demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.*

3. Atribuições e Responsabilidades

Todas as pessoas envolvidas (religiosas, diretores, lideranças, profissionais da saúde e demais pessoas colaboradoras) são responsáveis pelo cumprimento desta Política, e deverão utilizar, adequadamente, os dados pessoais em suas atividades, tanto no meio físico, quanto digital. É também responsabilidade de todas as pessoas se manterem atualizadas em relação a esta Política e aos procedimentos e normas relacionadas, bem como informar sobre eventual vulnerabilidade ou incidente detectado.

A fim de assegurar, em sua plenitude, o atendimento da proteção de dados pessoais previsto na LGPD, e, levando em conta as particularidades envolvendo o favorecimento da saúde, que mantém regulação própria, sua aplicação deve observar, além da LGPD, as normativas e regulamentações setoriais aplicáveis, dentre eles destaca-se: a) Confederação Nacional de Saúde (CNSaúde), a Agência Nacional de Saúde Suplementar (ANS), o Ministério da Saúde e os Conselhos Profissionais, no que tange à proteção dos dados pessoais dos pacientes, conforme Código de Boas Práticas – Proteção de Dados para Prestadores Privados em Saúde.

3.1. À Diretoria cabe:

- Prover os recursos necessários para a manutenção do Programa de Governança em Privacidade.
- Promover um ambiente seguro e saudável, que valorize a participação de todas as pessoas colaboradoras nas atividades relacionadas à privacidade e à proteção dos dados pessoais.

3.2. As lideranças deverão:

- Apoiar as ações dispostas no Programa de Governança em Privacidade de Dados Pessoais.
- Promover o engajamento da sua equipe e apoiar a divulgação desta Política e demais documentos que envolvam o tema.
- Revisar e manter atualizado o mapeamento de dados pessoais, pelo menos, uma vez a cada dois anos ou sempre que houver alteração no processo.
- Respeitar o titular do dado pessoal e gerar as evidências necessárias para apresentação às autoridades ou ao titular do dado pessoal, quando necessário.

3.3. O Comitê do Comitê de Privacidade e Proteção de Dados Pessoais deverá:

- Promover a divulgação desta Política e demais documentos, e tomar as ações necessárias para disseminar uma cultura de proteção aos dados pessoais dentro da organização.
- Manter monitoramento e manutenção constantes do Programa de Governança em Privacidade, de acordo com os requisitos da legislação aplicável.
- Acionar o encarregado pela Proteção de Dados Pessoais (DPO), sempre que necessário.
- Prever os recursos necessários para a manutenção do Programa de Governança em Privacidade.
- Incorporar a privacidade e a proteção de dados pessoais em todas as práticas de negócio promovidas pela organização.

- Realizar a avaliação dos prestadores de serviços, fornecedores e parceiros de negócios, especialmente quando operadores de dados pessoais, em relação ao atendimento às normas constantes na LGPD e suas regulamentações.
- Realizar treinamentos periódicos, a fim de promover a conscientização, o engajamento e a responsabilização das pessoas envolvidas com o tratamento de dados pessoais, em todos os níveis hierárquicos.

3.4. Os profissionais das áreas assistenciais, administrativas e de apoio deverão:

- Respeitar esta política e demais documentos relacionados à proteção de dados pessoais.
- Utilizar as informações ou dados pessoais de acordo com as finalidades determinadas pela RSDP.
- Adotar as medidas necessárias à proteção dos dados aos quais tiver acesso, direta ou indiretamente, em razão das suas atividades, mantendo o devido sigilo e confidencialidade.
- A equipe multidisciplinar de saúde deverá atentar e cumprir as determinações contidas nos Códigos de Ética dos respectivos Conselhos Profissionais, especialmente no tocante ao sigilo das informações contidas no prontuário do paciente/usuário.

3.5. A Equipe de Tecnologia da Informação deverá:

- Adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais, a fim de garantir alto nível de proteção para estes dados.
- Manter atualizadas as políticas, normas e procedimentos de segurança da informação.
- Tratar os eventuais incidentes de segurança da informação, envolvendo dados pessoais, de modo a garantir sua detecção, contenção, eliminação e recuperação.
- Apoiar o Comitê de Privacidade e Proteção de Dados Pessoais e a pessoa Encarregada da Proteção de Dados Pessoais (DPO), visando ao cumprimento integral do Programa de Governança em Privacidade, especialmente na comunicação com os titulares e as autoridades competentes, em casos de ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares.

3.6. Compete à pessoa Encarregada pelo Tratamento de Dados Pessoais (DPO):

- Orientar e apoiar o Comitê de Privacidade e Proteção de Dados Pessoais na elaboração do Programa de Governança em Privacidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.
- Aceitar reclamações e comunicações dos titulares de dados pessoais, prestar esclarecimentos e adotar as providências necessárias.
- Receber comunicações da Autoridade Nacional de Proteção de Dados (ANPD) e outras, esclarecimentos e indicar a adoção das providências necessárias.
- Propor medidas preventivas e corretivas necessárias para redução de eventual risco.

- Com base na legislação brasileira que regula o tratamento de dados pessoais, a LGPD – Lei Geral de Proteção de Dados Pessoais - Lei n°. 13.709/2018, informamos que a nossa Encarregada da Proteção de Dados Pessoais (DPO) é Stella Torresan Graeff, Coordenação da Área Jurídica da RSDP, disponível no e-mail dpo.rsdp@divinaprovidencia.org.br.

3.7. Área jurídica deve:

- Assegurar que os contratos com as pessoas colaboradoras, fornecedores e prestadores de serviços, operadores de dados pessoais, contenham cláusulas de proteção de dados pessoais adequadas à legislação e regulamentação aplicáveis;
- Prestar apoio jurídico na interpretação da legislação e regulamentação relativas à proteção de dados pessoais;
- Prestar apoio na ocorrência de incidentes envolvendo dados pessoais, em conjunto com a pessoa Encarregada da Proteção de Dados Pessoais (DPO).

4. Diretrizes

4.1 Diretrizes gerais

A RSDP seguirá as orientações dispostas nesta Política e demais documentos, realizando o tratamento dados pessoais e dados pessoais sensíveis em conformidade com as leis e regulamentações de proteção de dados pessoais, visando a, especialmente:

- Tratar os dados pessoais e os dados pessoais sensíveis de acordo com as hipóteses de tratamento previstas nos artigos 7º e 11 da LGPD.
- Garantir a transparência e a comunicação com o titular dos dados, especialmente em relação à realização da coleta dos dados pessoais e suas finalidades.
- Limitar a coleta, utilização, retenção, divulgação e compartilhamento de dados pessoais estritamente ao necessário para atingir a finalidade para o qual foram coletados.
- Garantir que a finalidade para o tratamento de dados pessoais seja específica e legítima.
- Garantir a qualidade e rastreabilidade dos dados pessoais durante todo o seu tratamento.
- Documentar e comunicar a todas as partes interessadas a respeito das políticas, procedimentos e práticas relacionadas à privacidade e proteção de dados.
- Melhorar continuamente o Programa de Governança em Privacidade de Dados Pessoais por meio de monitoramento, levando em conta os objetivos de privacidade e proteção de dados pessoais.
- Garantir que o tratamento de dados pessoais não seja usado para fins discriminatórios, ilícitos ou abusivos.
- Garantir que existam medidas de segurança adequadas e autorização da Diretoria para eventual transferência internacional de dados.

- Criar, revisar e comunicar diretrizes considerando melhores práticas para assegurar a proteção e privacidade dos dados pessoais.
- Promover, periodicamente, treinamentos e ações de conscientização a todos integrantes da organização, a fim de fomentar a cultura de segurança e reduzir possíveis riscos ao ambiente.
- Disseminar os Avisos de Privacidade da pessoa Colaboradora e do Cliente (Paciente/Usuário), de acordo com a categoria do titular, prezando pela transparência e pelo fornecimento de informações claras e acessíveis.

4.2 Dos dados pessoais sensíveis

- Observar, com cuidado adicional, e conferir proteção diferenciada aos dados pessoais considerados sensíveis, tendo em vista que o setor de saúde, pela sua própria natureza, realiza o tratamento destes dados em grande escala.
- Adotar medidas técnicas e administrativas voltadas para a proteção de tais informações, a fim de evitar divulgação e compartilhamento indevidos.
- Atentar que a tutela da saúde somente será aplicável aos tratamentos de dados pessoais que
forem realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária, não sendo aplicável a qualquer tratamento de dados pessoais realizado pela RSDP.

4.2.1 Dos Dados Pessoais de Crianças e Adolescentes

- Os dados pessoais de crianças e adolescentes deverão ser tratados visando ao seu melhor interesse, conforme art. 14 da LGPD.
- O tratamento de dados pessoais de crianças e adolescentes deverá ser realizado com o consentimento expresso, específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

4.3 Dos Agentes de Tratamento: Controlador e Operador

- Atentar para as especificidades de cada caso concreto e contexto, identificando a figura do Controlador e do Operador, com base na relação jurídica com o paciente/usuário. Para identificar o papel do prestador é necessário identificar a quem competem as decisões referentes ao tratamento de dados pessoais.
- Avaliar se o fornecedor, prestador de serviço ou parceiro de negócio contratado, operador de dados pessoais, possui requisitos mínimos de segurança e atende as determinações constantes
na LGPD.

4.4 Direito aos titulares de dados pessoais

A RSDP compromete-se a atender aos direitos dos titulares de dados pessoais, conforme previstos no artigo 17 a 19 da LGPD e demais normas pertinentes, os quais incluem:

- Criar e manter canais de comunicação para que os titulares dos dados tenham acesso facilitado às informações relacionadas aos seus dados pessoais.
- Possibilitar a portabilidade dos dados pessoais mediante requisição expressa do titular, com indicação de responsável técnico médico que irá recebê-los em meio eletrônico e sem custo ao cliente (paciente/usuário).
- Garantir, sempre que possível, que os titulares tenham a possibilidade de acessar e revisar seus dados pessoais, desde que sua identidade seja autenticada.
- Fornecer aos titulares dos dados pessoais tratados informações claras e facilmente acessíveis sobre as políticas, procedimentos e práticas com relação ao tratamento de dados pessoais realizado pela instituição.
- Informar os titulares de dados pessoais quando ocorrerem alterações significativas no tratamento dos seus dados pessoais.
- Eliminar de forma segura, bloquear ou anonimizar os dados pessoais após o término do seu ciclo de vida, observando as exigências legais e normativas sobre o tempo de retenção obrigatório.
- O atendimento ao direito do titular deverá seguir o Procedimento de Atendimento aos Titulares de Dados Pessoais determinado pela Autoridade Nacional de Proteção de Dados (ANPD).

4.5 Gerenciamento de incidente de dados pessoais e Comunicação à ANPD

Em caso de eventual incidente ou violação de dados pessoais que causem danos aos titulares, conforme definido pela ANPD, é essencial que seja feita adequada e tempestiva formalização do incidente, contendo o registro, a classificação, a forma de investigação, a correção, garantindo que todas as partes interessadas sejam notificadas, de acordo com o Procedimento em Caso de Incidente de Segurança com Dados Pessoais e Comunicação à ANPD, observada a abrangência legal definida.

4.6 Compartilhamento de informações contendo dados pessoais

- Apenas compartilhar informações dos pacientes conforme situações permitidas no Código de Ética Médica, nos seus artigos 54, 73 a 79 e 101, ou outros que venham a substituí-los;
- Cumprir a resolução do Conselho Federal de Medicina (CFM) n° 1.605, de 15 de setembro de 2000, ou outras similares, quando se tratar da necessidade de consentimento para o compartilhamento de informação do prontuário e ficha médica.
- Anonimizar informações de pacientes/usuários ao compartilhá-las com outros profissionais para dirimir dúvidas, obter uma segunda opinião sobre determinado diagnóstico ou outras finalidades diretamente relacionadas à tutela da saúde do paciente/usuário.

- Seguir o parecer n° 14/2017 do CFM, ou outras normativas que venham a regulamentar a matéria, quanto ao uso do WhatsApp e demais plataformas de comunicação.
- Seguir o protocolo TISS, regulamentado pela Resolução Normativa da ANS n° 305/2012, ou outra que vier a substitui-la, quando o compartilhamento for com agentes de saúde suplementar.
- Buscar o consentimento do paciente/usuário para autorizar o compartilhamento de seus dados pessoais sensíveis quando a finalidade não for para cumprimento legal ou regulatório.

4.7 Armazenamento de dados pessoais

4.7.1 Armazenamento de dados pessoais de clientes (pacientes/usuários) e/ou responsáveis legais

Armazenar os dados pessoais referentes à saúde do paciente/usuário e seu prontuário por no mínimo 20 anos, e no que se refere à digitalização e à utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente, conforme previsto na Lei no 13.787/2018 e na Resolução CFM no 1.821/2007, ou em outras normas que venham a substitui-las.
Os dados pessoais meramente administrativos devem ser armazenados pelo período necessário ao cumprimento da finalidade para a qual foram coletados e/ou conforme previsto em legislação própria.

4.7.2 Armazenamento de dados pessoais de profissionais da saúde, administrativos e de apoio

Os documentos referentes aos profissionais da saúde, administrativos e de apoio deverão atender ao prazo de armazenamento previsto na legislação trabalhista e/ou outras aplicáveis.

4.8 Eliminação de dados pessoais

Eliminar os dados pessoais de forma a resguardar a intimidade do titular e o sigilo das informações, em atendimento aos artigos 15 e 16 da LGPD, ou outros que venham a substitui-los, que indicam que o término do tratamento dos dados pessoais está condicionado ao alcance da(s) finalidade(s), levando-se em conta, também, as respectivas bases legais aplicáveis.
Buscar, sistematicamente, as melhores práticas para eliminação de dados pessoais, tanto em meios físicos quanto digitais. Se necessário, buscar apoio do setor de TI e/ou da pessoa Encarregada pela Proteção de Dados Pessoais (DPO).

5. Documentos de referência

- Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018,
- Mapeamento de Dados Pessoais da RSDP,
- Aviso de privacidade do Cliente (Paciente/Usuário), Aviso de Privacidade das Pessoas Colaboradoras,
- Procedimento de Atendimento aos Titulares de Dados Pessoais (Fluxograma), Procedimento em Caso de Incidente de Segurança com Dados Pessoais e Comunicação à ANPD, Relatório de Impacto de Proteção de Dados Pessoais – RIPD,
- Política de Segurança e Privacidade da Informação RSDP/INST/POL 0016,
- Código de Conduta RSDP/INST/CC 002.

VI. DISPOSIÇÕES GERAIS

É dever de todas as pessoas colaboradoras da RSDP observar, integralmente, os termos desta Política e as demais normas internas que venham a regular a proteção de dados pessoais. Caso haja violação das regras estabelecidas, a instituição poderá aplicar as sanções disciplinares cabíveis, de acordo com a gravidade da ocorrência.

VII. REFERÊNCIAS (FACULTATIVO)

- Código de Boas Práticas: Proteção de Dados para Prestadores Privados de Serviços em Saúde, Confederação Nacional de Saúde (CNSaúde), 2021.
- Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, Autoridade Nacional de Proteção de Dados (ANPD), 2022.
- Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018.

CRÉDITO: Esta política foi elaborada pela DPOfficer brazil® e validada pelo Comitê de Privacidade e Proteção de Dados Pessoais da RSDP, na data de 12 de abril de 2024.