FIOTEC
FIOCRUZ

POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Sumário

1 Apresentação

Esta política integra o Sistema de Informação Documentada da Fundação para o Desenvolvimento Científico e Tecnológico em Saúde (Fiotec), e nela, assumimos o compromisso institucional com a privacidade e proteção de dados pessoais, como valor fundamental em suas operações.

Esta Política estabelece diretrizes para o tratamento de dados pessoais, em conformidade com a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) e com as melhores práticas nacionais e internacionais recomendadas por entidades reguladoras.

2 Finalidade

Esta política tem como finalidades:

- Definir normas claras e abrangentes para o tratamento ético, seguro e legal de dados pessoais coletados, processados e armazenados pela Fiotec;
- Estabelecer diretrizes para garantir a privacidade e os direitos dos titulares dos dados pessoais;
- Assegurar a conformidade com a LGPD e outras regulamentações aplicáveis;
- Promover uma cultura organizacional orientada à privacidade e proteção de dados pessoais;
- Construir e manter relações de confiança com os titulares dos dados e demais partes interessadas;
- Mitigar riscos relacionados a violações de privacidade e possíveis sanções legais.

3 Aplicabilidade

Esta Política é aplicável a:

- Todos os colaboradores da Fiotec, incluindo empregados com vínculo CLT, estagiários, bolsistas, pesquisadores, diretores e conselheiros;

- Prestadores de serviços, consultores, fornecedores e terceirizados que tenham acesso ou realizem tratamento de dados pessoais em nome da Fiotec;
- Todos os ambientes físicos e digitais da organização, incluindo sistemas, redes, dispositivos corporativos, aplicativos móveis e instalações onde ocorra tratamento de dados pessoais;

4 Princípios

A Política segue os princípios fundamentais da LGPD e melhores práticas internacionais como a ISO/IEC 27701:

a) **Transparência e informação**: garantia de informações claras, precisas e acessíveis aos titulares sobre o tratamento de seus dados pessoais.
b) **Finalidade específica**: realização do tratamento para propósitos legítimos, específicos e explícitos informados ao titular.
c) **Adequação, necessidade e minimização**: tratamento compatível com as finalidades informadas e limitado ao mínimo necessário para alcançá-las.
d) **Livre acesso**: garantia de consulta facilitada e gratuita pelos titulares sobre o tratamento de seus dados.
e) **Qualidade dos dados**: garantia de exatidão, clareza, relevância e atualização dos dados.
f) **Segurança e prevenção**: adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais e prevenir danos aos titulares.
g) **Não discriminação**: impossibilidade de tratamento para fins discriminatórios, ilícitos ou abusivos.
h) **Responsabilização e prestação de contas**: demonstração da adoção de medidas eficazes para cumprir as normas de proteção de dados.
i) **Limitação de armazenamento**: manutenção dos dados apenas pelo tempo necessário para cumprir as finalidades do tratamento.

5 Conteúdo

5.1 Bases Legais para o Tratamento

a) Todo tratamento de dados pessoais deve ser fundamentado em pelo menos uma das bases legais previstas na LGPD (Art. 7º e 11º).
b) A base legal utilizada deve ser claramente identificada, documentada e comunicada aos titulares de dados.
c) Para dados pessoais sensíveis, observar as bases legais específicas e limitadas previstas no Art. 11 da LGPD.

5.2 Controle de Acesso

a) O acesso aos dados pessoais deve ser restrito a colaboradores autorizados, conforme suas funções e responsabilidades específicas.
b) Devem ser implementados controles técnicos de acesso, incluindo autenticação multifator para sistemas que processam dados sensíveis
c) Revisões periódicas dos privilégios de acesso devem ser realizadas, no mínimo, a cada seis meses.

5.3 Segurança da Informação

Toda atividade que envolva dados pessoais na Fiotec deve adotar medidas de segurança compatíveis com os riscos envolvidos, incluindo controle de acessos, proteção contra vazamentos, criptografia e resposta a incidentes.
Esses princípios seguem as diretrizes definidas na Política de Segurança da Informação (PSI), documento publicado que detalha os controles técnicos e administrativos obrigatórios para todos os sistemas e áreas.
Além disso, a Fiotec possui a Norma de Tratamento de Incidentes de Segurança da Informação, assegurando que, diante de um incidente, sejam adotadas medidas adequadas de contenção, investigação, comunicação e correção, em conformidade com a Lei Geral de Proteção de Dados (LGPD).

5.4 Transparência

a) A Fiotec deve manter um aviso de privacidade atualizado e de fácil acesso, detalhando as práticas de tratamento de dados pessoais.
b) Avisos de privacidade específicos devem ser fornecidos sempre que novos dados pessoais forem coletados.
c) Deve-se garantir linguagem clara e acessível em todas as comunicações sobre privacidade.

5.5 Ciclo de Vida dos Dados Pessoais

5.5.1 Coleta

a) A coleta de dados pessoais deve limitar-se ao mínimo necessário para atender à finalidade específica.
b) No momento da coleta, o titular deve ser informado sobre: finalidade, forma e duração do tratamento, identificação do controlador, informações de contato do DPO, direitos do titular e possíveis compartilhamentos.
c) Deve-se obter consentimento específico para coleta de dados de crianças e adolescentes, conforme Art. 14 da LGPD.

5.5.2 Tratamento (Processamento)

a) O processamento dos dados deve ser restrito às finalidades informadas ao titular.
b) Quando aplicável, implementar técnicas de pseudonimização ou anonimização para reduzir riscos aos titulares.
c) Manter registros detalhados de todas as operações de tratamento realizadas (RIPD - Relatório de Impacto à Proteção de Dados) que possam trazer riscos significativos aos titulares.

5.5.3 Armazenamento

a) Estabelecer prazos de retenção específicos para cada categoria de dados pessoais, com base em requisitos legais, contratuais e operacionais.
b) Implementar processo de revisão periódica para identificar e eliminar dados que já cumpriram sua finalidade ou excederam o prazo de retenção necessário.
c) Garantir que ambientes de desenvolvimento e testes utilizem dados anonimizados ou fictícios.

5.5.4 Eliminação

a) Desenvolver procedimentos seguros para eliminação dos dados após cumprimento da finalidade ou por solicitação do titular.
b) A eliminação deve garantir que os dados não possam ser recuperados, utilizando técnicas apropriadas como exclusão segura ou destruição física de mídias.
c) Documentar todas as eliminações de dados para fins de auditoria e conformidade.
d) Toda solicitação de eliminação por parte do titular deve ser processada conforme os prazos estabelecidos pela LGPD.

5.6 Direitos dos Titulares

A Fiotec deve garantir o exercício dos seguintes direitos dos titulares:

a) **Confirmação e acesso**: fornecer informações sobre a existência de tratamento e permitir acesso aos dados.
b) **Correção**: possibilitar a atualização de dados incompletos, inexatos ou desatualizados.

c) **Anonimização/Bloqueio/Eliminação**: processar solicitações relacionadas a dados desnecessários, excessivos ou tratados em desconformidade com a LGPD.
d) **Revogação do consentimento**: possibilitar a revogação do consentimento a qualquer momento.
e) **Informação sobre compartilhamento**: informar entidades públicas e privadas com as quais os dados foram compartilhados.
f) **Informação sobre consequências**: esclarecer consequências de não fornecer consentimento quando solicitado.

Para atender a estas demandas, a Fiotec disponibiliza os seguintes canais para exercício dos direitos dos titulares:

- Formulário eletrônico disponível no portal institucional (https://www.fiotec.fiocruz.br/contato-lgpd)
- E-mail dedicado: privacidade@fiotec.fiocruz.br
- Atendimento presencial mediante agendamento prévio

Todas as solicitações serão registradas em sistema próprio e terão prazo máximo de resposta de 15 dias úteis, com possibilidade de prorrogação justificada por igual período. O titular será informado sobre o andamento de sua solicitação durante todo o processo.

5.7 Transferências Internacionais

5.7.1 Requisitos para Transferências

a) Transferências internacionais de dados pessoais somente serão permitidas para países ou organismos que proporcionem grau de proteção adequado, conforme definido pela ANPD.
b) Na ausência de nível adequado de proteção, as transferências só poderão ocorrer mediante análise prévia e aprovação da Alta Direção.

5.8 Matriz de Responsabilidades

Responsável	Atividade
BÁSICO	
Todos os Colaboradores da Fiotec	• Conhecer e cumprir as diretrizes desta Política, assim como comunicar qualquer violação ou suspeita, por meio dos canais disponibilizados pela Fiotec; • Participar dos treinamentos obrigatórios sobre privacidade e proteção de dados; • Assinar termo de ciência e responsabilidade após cada treinamento, que será arquivado pelo Departamento de Recursos Humanos. • Comunicar imediatamente qualquer suspeita ou ocorrência de violação à privacidade e segurança dos dados pessoais; • Adotar o princípio de "Privacy by Design" em todas as atividades que envolvam dados pessoais.
Gestores da Fiotec	• Garantir na sua equipe a leitura e a aplicação do conteúdo desta Política; • Assegurar que os princípios e diretrizes orientem permanentemente as decisões de suas equipes; • Garantir que contratos com terceiros incluam cláusulas específicas sobre proteção de dados.
Diretoria Executiva	• Aprovar o conteúdo dessa Política; • Garantir a aplicação desta Política;
Conselho Curador	• Aprovar o conteúdo dessa Política.

ESPECÍFICA	
Coordenação de Segurança da Informação	• Promover a cultura de Privacidade e Proteção de Dados na Instituição; • Prover recursos técnicos para execução dessa Política; • Revisão periódica desta Política; • Tratar incidentes que violem esta Política.
Comitê de Segurança da Informação e Privacidade	• Aprovar o conteúdo e garantir a aplicação dessa Política; • Deliberar sobre questões estratégicas relacionadas à privacidade e proteção de dados; • Acompanhar respostas a incidentes e coordenar comunicação interna e externa; • Acompanhar, avaliar, propor alterações, dirimir eventuais dúvidas e deliberar sobre os assuntos abordados nessa Política. • Deliberar sobre RIPDs de projetos de alto risco.
Encarregado de Dados (DPO)	• Atuar como canal de comunicação entre a Fiotec, os titulares dos dados e a ANPD; • Orientar colaboradores sobre práticas a serem adotadas em relação à proteção de dados; • Executar demais atribuições determinadas pela Fiotec ou estabelecidas em normas complementares. • Reportar regularmente à alta direção sobre o status de conformidade da organização. • Acompanhar a revisão anual desta política, que será formalmente aprovada pela Diretoria

	Executiva, com registro documentado das revisões e alterações efetuadas.
Assessoria de Planejamento e Qualidade	• Revisar e publicar este documento.

6 Disposições Gerais

I. O descumprimento das diretrizes descritas nesta política constitui violação grave, sujeitando os responsáveis a sanções, conforme a gravidade da infração.

II. A graduação das sanções seguirá os critérios de proporcionalidade, reincidência, dolo ou culpa, e extensão do dano causado.

III. Esta política deve ser interpretada em conjunto com o Código de Conduta Ética da Fiotec e demais políticas internas.

IV. Em caso de dúvidas ou conflito entre esta política e requisitos legais ou contratuais específicos, consultar o DPO ou o Comitê de Segurança da Informação e Privacidade.

V. A Fiotec reserva-se o direito de monitorar o cumprimento desta política através de auditorias periódicas.

7 Referências Normativas

- Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/2018)
- Normas e orientações da Autoridade Nacional de Proteção de Dados (ANPD)
- ISO/IEC 27701:2019 - Extensão da ISO/IEC 27001 e ISO/IEC 27002 para gestão da privacidade da informação

Documentos Internos Complementares:

- Política de Segurança da Informação
- Código de Conduta Ética da Fiotec

8 Controles e Revisões

Revisão	Data	Resumo da Alteração
0	10/09/2025	Versão Inicialaprovada pela Diretoria e Conselho Curador

9 Termos e Definições

- **Anonimização**: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (definição conforme Art. 5º, XI da LGPD).

- **ANPD**: Autoridade Nacional de Proteção de Dados, órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional (definição conforme Art. 5º, XIX da LGPD).

- **Consentimento**: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

- **Controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

- **Dado pessoal**: informação relacionada a pessoa natural identificada ou identificável.

- **Dado pessoal sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização religiosa, filosófica ou política, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

- **DPO (Data Protection Officer)**: encarregado pelo tratamento de dados pessoais, responsável por atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

- **Operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

- **Pseudonimização**: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente.

- **RIPD**: Relatório de Impacto à Proteção de Dados Pessoais, documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais.

- **Titular dos dados**: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

- **Transferência internacional de dados:** transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

- **Tratamento**: toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, modificação, comunicação, transferência, difusão ou extração.

10 Anexos

Não se aplica