



POLÍTICA DE GESTÃO E PROTEÇÃO DA INFORMAÇÃO



GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria da Saúde



SUMÁRIO

1 Finalidade.....	3
2 Abrangência	3
3 Regulação	3
4 Definições técnicas	4
5 Princípios.....	5
6 Do Tratamento dos Dados Pessoais.....	5
7 Medidas de segurança	7
8 Direitos do titular	11
9 Responsabilidades.....	11
10 Estrutura de Governança Digital e Gestão da Proteção de Dados	14
11 Relatório de Impacto à Proteção de Dados Pessoais (RIPD).....	14
12 Sanções e Penalidades	16
13 Disposições Finais	16

POLÍTICA	
Título: Política de Gestão e Proteção da Informação	Código: POL.013
	Revisão: 0

POLÍTICA DE GESTÃO E PROTEÇÃO DA INFORMAÇÃO

APROVAÇÃO PERANTE O CONSELHO CURADOR

A presente Política foi aprovada pelo Conselho Curador da Fundação Estadual de Inovação em Saúde - iNOVA Capixaba, em 18/08/2026 – ata da 4ª Reunião do Conselho Curador – em sessão Ordinária.

1 FINALIDADE

A presente Política de Gestão e Proteção da Informação é instituída com a finalidade de formalizar e consolidar o compromisso institucional da Fundação iNOVA Capixaba com a observância às normas aplicáveis à proteção de dados pessoais e privacidade, bem como com a gestão segura, eficiente e integrada das informações utilizadas em seus processos administrativos, assistenciais e estratégicos.

2 ABRANGÊNCIA

A Política de Gestão e Proteção da Informação aplica-se à Fundação Estadual de Inovação em Saúde - iNOVA Capixaba – em toda sua estrutura organizacional: hospital próprio, filiais, unidades gestoras, administrativas e assistenciais, escritórios, ou representações – aos gestores, empregados, colaboradores, servidores cedidos, prestadores de serviços e demais partes interessadas.

3 REGULAÇÃO

3.1 Esta política fundamenta-se nos seguintes instrumentos legais e normativos:

- Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- Código de Ética, Conduta e Integridade iNOVA Capixaba;
- Manual Brasileiro de Acreditação – Organização Nacional de Acreditação (ONA);
- Lei nº 12.527/2011 – Lei de Acesso à Informação.

3.2 Esta Política articula-se com a Política de Comunicação Institucional da Fundação. As disposições desta Política prevalecem em matéria de proteção de dados pessoais, segurança da informação, classificação da informação e notificação de incidentes; os aspectos comunicacionais, reputacionais e de relacionamento institucional decorrentes observarão a Política de Comunicação Institucional.

4 DEFINIÇÕES TÉCNICAS

4.1 Os termos técnicos utilizados nesta Política possuem as definições dispostas nos seguintes itens:

4.1.1 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;

4.1.2 banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

4.1.3 consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

4.1.4 controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais;

4.1.5 Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável;

4.1.6 Dado Pessoal Sensível: dado pessoal sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter sigiloso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

4.1.7 Dado Anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

4.1.8 Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

4.1.9 Encarregado: colaborador da iNOVA Capixaba formalmente designado pelo Diretor-Geral da Fundação, ou agente externo de natureza física ou jurídica especialmente contratado, que atua como canal de comunicação entre a Fundação, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

4.1.10 Titular: pessoa física ou natural a quem se referem os dados pessoais que são objeto de tratamento;

4.1.11 Tratamento: toda operação realizada com dados pessoais, 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;

4.1.12 Transferência Internacional De Dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

4.1.13 Uso Compartilhado De Dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de banco de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

4.1.14 operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

4.1.15 Relatório de Impacto à Proteção De Dados Pessoais (RIPD): documentação padronizada da Fundação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de riscos.

5 PRINCÍPIOS

5.1 A Política observará os seguintes princípios:

5.1.1 Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

5.1.2 Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

5.1.3 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;

5.1.4 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;

5.1.5 Não Discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

5.1.6 Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

5.1.7 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;

5.1.8 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;

5.1.9 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;

5.1.10 Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.

6 DO TRATAMENTO DOS DADOS PESSOAIS

6.1 Coleta

6.1.1 A coleta de dados pessoais é essencial para a correta prestação dos serviços voltados à área da saúde que a Fundação iNOVA Capixaba se propõe, contemplando a assistência, o ensino, a pesquisa e as atividades administrativas decorrentes.

6.1.2 Os dados pessoais poderão ser recolhidos através do atendimento presencial ou virtual ao usuário; na prestação de serviços de assistência médica e no sítio eletrônico da Fundação.

6.1.3 A coleta também poderá ocorrer por meio de pesquisas, quando na condição de participante, assinar o respectivo Termo de Consentimento. Nos casos envolvendo pesquisas, todo o projeto será previamente submetido à Comissão Interna de Ética e Pesquisa (COMISEP). Caberá à COMISEP analisar criteriosamente todos os estudos propostos que envolvam dados pessoais e dados pessoais sensíveis.

6.2 Compartilhamento

6.2.1 Os dados pessoais poderão ser compartilhados com órgãos e entidades da Administração Pública, bem como com instituições privadas que mantenham relação contratual, convênio ou instrumento congênere com a Fundação, observados os princípios de finalidade, necessidade e adequação.

6.2.2 Poderá ocorrer a transferência internacional de dados pessoais e dados pessoais sensíveis, quando necessária à execução de atividades institucionais, assistenciais, administrativas ou científicas, observadas as disposições da LGPD e demais normas aplicáveis.

6.2.3 O compartilhamento de dados pessoais e dados pessoais sensíveis, no âmbito nacional ou internacional, com terceiros contratados ou parceiros institucionais, será obrigatoriamente precedido da celebração de instrumentos jurídicos que contenham cláusulas específicas de confidencialidade, proteção de dados e segurança da informação compatíveis com a natureza e a sensibilidade das informações tratadas.

6.2.4 Os dados pessoais deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado nos termos da LGPD, de forma a facilitar seu uso quando necessário.

6.3 Eliminação

6.3.1 Após o cumprimento da finalidade que justificou o tratamento e esgotado o prazo de guarda previsto em norma legal, os dados pessoais serão eliminados ou terão sua destinação definida de acordo com os critérios estabelecidos em regulamento arquivístico interno – Plano de Classificação de Documentos e Tabela de Temporalidade.

6.3.2 É assegurado ao titular dos dados o direito de requerer a exclusão de seus dados pessoais ou de se opor ao tratamento realizado. Não obstante, o pleito poderá ser legitimamente indeferido quando houver fundamento jurídico que autorize ou imponha a manutenção do tratamento ou guarda dos dados pessoais, notadamente para o cumprimento de obrigação legal ou regulatória.

6.3.3 Os prazos de retenção definidos no instrumento referido no item 6.3.1 observarão, além da finalidade que justificou o tratamento, as obrigações legais e regulatórias específicas do setor de saúde, em especial:

I — a Lei nº 13.787/2018, que dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente;

II — as resoluções do Conselho Federal de Medicina que disciplinam os prazos mínimos de conservação de prontuários e demais documentos médicos;

III — as normas expedidas pelos órgãos reguladores setoriais, quando aplicáveis à atuação da Fundação.

6.3.4 Em caso de conflito entre os prazos estabelecidos na Tabela de Temporalidade e aqueles fixados pelos normativos referidos no item anterior, prevalecerá o prazo mais longo que seja legalmente exigível, assegurando a integridade das informações.

6.4 Finalidade

6.4.1 Os dados pessoais e os dados pessoais sensíveis, inclusive aqueles direta ou indiretamente relacionados à prestação de serviços de saúde, serão tratados para o desempenho das atividades institucionais, compreendendo a assistência, o ensino, a pesquisa e as atividades administrativas correlatas.

6.5 Tratamento de Dados Pessoais de Crianças e Adolescentes

6.5.1 O tratamento de dados pessoais de crianças e adolescentes pela Fundação iNOVA Capixaba será realizado exclusivamente em seu melhor interesse, em conformidade com o art. 14 da Lei nº 13.709/2018.

6.5.2 O tratamento de dados pessoais de crianças e adolescentes será realizado em observância ao seu melhor interesse e às bases legais previstas na LGPD, podendo fundamentar-se, conforme o caso concreto, no consentimento do responsável legal, na tutela da saúde, na proteção da vida ou da incolumidade física do titular ou de terceiros, no cumprimento de obrigação legal ou regulatória, bem como na execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres celebrados pela Administração Pública.

6.5.3 No contexto assistencial, quando a urgência ou a emergência clínica não permitir a obtenção prévia do consentimento do responsável legal, o tratamento dos dados do menor será realizado com fundamento na proteção de sua vida e saúde, devendo o consentimento ser obtido tão logo as circunstâncias o permitam.

6.5.4 O tratamento de dados pessoais de crianças e adolescentes que apresente potencial risco ou impacto relevante à privacidade ensejará obrigatoriamente a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), conforme o item 11.2, V, desta Política.

7 MEDIDAS DE SEGURANÇA

7.1 Controle de Acesso, Identidade e Infraestrutura

7.1.1 Será adotado controle de acesso baseado em perfis (RBAC). Os acessos serão concedidos mediante autenticação segura, podendo incluir múltiplos fatores de autenticação (MFA), conforme criticidade do sistema. Os acessos serão revisados periodicamente e imediatamente revogados em caso de desligamento ou mudança de função.

7.1.2 Os sistemas desenvolvidos ou contratados, utilizados pela Fundação para o tratamento de dados pessoais serão estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD e nas diretrizes fixadas pela ANPD e serão concebidos segundo a abordagem de privacidade desde a concepção (*privacy by design*) e como padrão de sistemas e práticas de negócios.

7.1.3 A Gerência de Tecnologia da Informação e Comunicação (GTIC) adotará e proporá a adoção de medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito, observando padrões técnicos mínimos definidos pela ANPD.

7.1.4 Os setores da Fundação, o encarregado e o setor de Governança Digital e Gestão da Proteção de Dados, no âmbito de suas competências, poderão estabelecer regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais, observado o disposto no art. 50 da LGPD.

7.1.5 Os setores da Fundação deverão comunicar imediatamente ao encarregado e ao setor de Governança Digital e Gestão da Proteção de Dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, para fins do disposto no inciso VIII do item 9.3 desta Política. Quando o incidente caracterizar cenário de crise institucional, o fluxo de notificação de que trata este item será conduzido de forma articulada com a Política de Comunicação Institucional, cabendo a esta Política a coordenação da notificação ao titular e à ANPD nos prazos legais, independentemente da deliberação do Comitê de Crise.

7.1.6 Adicionalmente, o acesso aos dados pessoais e dados pessoais sensíveis será restrito a colaboradores, servidores cedidos, prestadores de serviços e outras pessoas devidamente autorizadas, limitando-se às hipóteses em que o conhecimento das informações seja estritamente necessário ao desempenho de suas atribuições funcionais.

7.1.7 Os dados pessoais sensíveis deverão ser protegidos por mecanismos de criptografia em repouso e em trânsito e, sempre que possível, serão aplicadas técnicas de anonimização ou pseudonimização, sendo adotada política de classificação da informação, definindo níveis de criticidade e proteção;

7.1.8 A infraestrutura de TI contará com mecanismos de proteção como *firewall*, sistemas de detecção e prevenção de intrusão (IDS/IPS) e segmentação de rede, cujos ambientes serão monitorados continuamente quanto a eventos de segurança.

7.1.9 Serão mantidos registros de logs de acesso, alteração e exclusão de dados, protegidos contra alteração e mantidos pelo período definido em normativo interno.

7.1.10 Serão realizados *backups* periódicos dos dados, com armazenamento seguro e segregado, devendo ser realizados testes de restauração regularmente;

7.2 Classificação da Informação

7.2.1 As informações produzidas, recebidas ou custodiadas pela Fundação iNOVA Capixaba serão classificadas segundo seu grau de sensibilidade e restrição de acesso, observando-se os seguintes níveis:

I — Pública: informação cuja divulgação não acarreta riscos à Fundação ou a terceiros, podendo ser acessada por qualquer pessoa, interna ou externamente;

II — Interna: informação de uso restrito ao âmbito da Fundação, cujo acesso por pessoas externas, sem autorização, pode causar inconveniências operacionais ou administrativas;

III — Confidencial: informação sensível cujo acesso deve ser limitado a colaboradores, servidores e prestadores com necessidade funcional comprovada, e cuja divulgação não autorizada pode acarretar danos à Fundação, a parceiros institucionais ou a titulares de dados;

IV — Restrita: informação de mais alto grau de sigilo, incluindo dados pessoais sensíveis, informações estratégicas, segredos operacionais e documentos sujeitos a sigilo legal ou regulatório, cujo acesso é permitido apenas a pessoas expressamente autorizadas pelo Diretor-Geral ou por ele delegadas.

7.2.2 A classificação da informação deverá ser realizada pelo responsável pela área que a produz ou custodia, com base nos critérios estabelecidos nesta Política e em normativo interno específico a ser aprovado pelo Diretor-Geral da Fundação.

7.2.3 A reclassificação ou desclassificação de informações seguirá os mesmos critérios e competências previstos no item anterior, devendo ser formalizada e registrada.

7.2.4 O descarte de informações classificadas observará procedimentos que garantam a eliminação segura e irreversível do conteúdo, conforme as diretrizes do regulamento arquivístico interno referido no item 6.3.1.

7.3 Obtenção, Análise e Validação da Informação

7.3.1 A Fundação iNOVA Capixaba adotará métodos estruturados de obtenção, análise e validação das informações necessárias ao monitoramento de seus resultados institucionais e ao apoio às decisões administrativas, assistenciais e estratégicas.

7.3.2 As principais fontes de informação utilizadas nos processos decisórios da Fundação incluem:

I — sistemas de informação em saúde e prontuários eletrônicos de pacientes, para o monitoramento da produção e da qualidade assistencial;

II — sistemas administrativos e financeiros, para o acompanhamento da execução orçamentária e da gestão de contratos;

III — indicadores de desempenho institucionais, produzidos periodicamente pelas unidades organizacionais competentes e consolidados pela gerência de cada setor, com apoio do setor de Qualidade;

IV — relatórios de auditoria interna e de órgãos externos de controle, para fins de avaliação de conformidade e de melhoria contínua dos processos.

7.3.3 As informações utilizadas em processos decisórios deverão ser validadas quanto à sua exatidão, completude e atualidade antes de servirem de base para deliberações formais, cabendo ao responsável pela área que as produziu atestar sua confiabilidade.

7.3.4 A Gerência de Tecnologia da Informação e Comunicação (GTIC) apoiará a disponibilização de informações íntegras e tempestivas, por meio da manutenção e da atualização dos sistemas de informação utilizados pela Fundação, assegurando a rastreabilidade das operações realizadas.

7.3.5 Os indicadores de qualidade e de desempenho institucional serão revisados periodicamente, com periodicidade mínima anual, podendo ser alterados por decisão da Diretoria Executiva da Fundação.

7.4 Capacitação em Segurança e Tecnologia da Informação

7.4.1 A Fundação iNOVA Capixaba promoverá programa estruturado de capacitação de seus colaboradores, servidores cedidos e prestadores de serviços habituais sobre o uso adequado das tecnologias da informação, a segurança de dados e as obrigações decorrentes desta Política e da legislação de proteção de dados.

7.4.2 O programa de capacitação abrangerá, no mínimo, os seguintes temas:

I — princípios e obrigações da Lei nº 13.709/2018 (LGPD), com ênfase nas responsabilidades dos colaboradores no tratamento de dados pessoais;

II — classificação da informação e procedimentos de manuseio, armazenamento e descarte seguros;

III — reconhecimento e comunicação de incidentes de segurança da informação;

IV — boas práticas no uso de dispositivos, sistemas e redes institucionais, incluindo a prevenção de ataques de engenharia social e *phishing*;

V — regras de controle de acesso, uso de senhas e autenticação multifator, caso aplicáveis.

7.4.3 As ações de capacitação serão organizadas pela Gerência de Tecnologia da Informação e Comunicação (GTIC) em conjunto com a área de Controladoria e Integridade (CT) e com o Encarregado pelo tratamento de dados pessoais, com periodicidade mínima anual, podendo ser realizadas em formato presencial, remoto ou híbrido, conforme as necessidades institucionais.

7.4.4 A participação nas capacitações de que trata este item será obrigatória para todos os colaboradores, servidores cedidos e prestadores que, em razão de suas funções, acessem sistemas ou bases de dados da Fundação, devendo ser registrada em instrumento próprio para fins de comprovação e controle.

7.5 Plano de Recuperação de Desastres

7.5.1 A Fundação iNOVA Capixaba manterá Plano de Recuperação de Desastres (PRD) formalmente documentado, destinado a assegurar a continuidade operacional dos sistemas e processos críticos em situações de falha grave, desastre tecnológico, incidente de segurança de grande impacto ou indisponibilidade prolongada da infraestrutura de tecnologia da informação.

7.5.2 O Plano de Recuperação de Desastres deverá contemplar, no mínimo:

I — identificação e priorização dos sistemas de informação, bases de dados e processos considerados críticos para a continuidade das atividades assistenciais, administrativas e estratégicas da Fundação;

II — definição dos objetivos de tempo de recuperação (*RTO — Recovery Time Objective*) e de ponto de recuperação (*RPO — Recovery Point Objective*) para cada sistema ou conjunto de dados críticos;

III — descrição dos procedimentos de ativação do plano, com identificação dos responsáveis por cada etapa e dos critérios que caracterizam situação de desastre para fins de sua aplicação;

IV — definição das estratégias de recuperação, incluindo o uso de ambientes alternativos de processamento e os procedimentos de restauração a partir dos backups realizados nos termos do item 7.1.10;

V — procedimentos de comunicação interna e externa durante a ocorrência do desastre, abrangendo a notificação à Diretoria-Geral, às áreas afetadas e, quando aplicável, aos titulares de dados e à ANPD.

7.5.3 O Plano de Recuperação de Desastres será elaborado e mantido pela Gerência de Tecnologia da Informação e Comunicação (GTIC), com aprovação do Diretor-Geral da Fundação, e revisado sempre que ocorrerem alterações relevantes na infraestrutura tecnológica ou nos processos institucionais.

7.5.4 Serão realizados testes periódicos do Plano de Recuperação de Desastres, com periodicidade mínima anual, cujos resultados serão documentados e utilizados para aprimoramento contínuo das estratégias e procedimentos nele previstos.

8 DIREITOS DO TITULAR

8.1 Nos termos da legislação aplicável, o titular poderá, a qualquer momento requerer:

- a. Confirmação da existência de tratamento de dados;
- b. Acesso aos dados que lhe digam respeito;
- c. Correção de dados incompletos, inexatos ou desatualizados;
- d. Anonimização, bloqueio ou eliminação de dados excessivos ou que estejam sendo tratados ilícitamente;
- e. Portabilidade dos dados a outro fornecedor de serviço ou produto, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- f. Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD;
- g. Informação sobre o compartilhamento de seus dados com entes públicos e privados, caso exista;
- h. Informação sobre a opção de não autorizar o tratamento de seus dados e as consequências da negativa;
- i. Revogação do consentimento, excetuando-se as hipóteses previstas na legislação vigente;
- j. Oposição ao tratamento realizado em desconformidade com as determinações da LGPD;
- k. Peticionar em relação ao tratamento dos seus dados pessoais à Autoridade Nacional de Proteção de Dados Pessoais;
- l. Revisão de decisões tomadas unicamente com base em tratamento automatizado de Dados Pessoais que afetem seus interesses.

9 RESPONSABILIDADES

9.1 Na Fundação iNOVA Capixaba, são considerados como titulares de dados:

- Colaboradores, concursados, servidores cedidos, designação temporária, ocupantes de cargos de confiança, recrutamento amplo, processo seletivo, que se encontrem desempenhando suas atividades no âmbito da Fundação iNOVA Capixaba;
- Pacientes, seus responsáveis legais e acompanhantes;
- Estudantes, estagiários, residentes, professores e pesquisadores;
- Profissionais de empresas terceirizadas e todos aqueles que, de forma individual ou coletiva, por força de lei, contrato, convênio ou qualquer outro instrumento jurídico, se

relacionam ou atuem na prestação de serviços à Fundação iNOVA Capixaba ou suas filiais, de natureza permanente, temporária ou excepcional, ainda que sem retribuição financeira, direta ou indiretamente;

- Outras pessoas que tiverem seus dados pessoais sob os cuidados, ainda que temporariamente, da Fundação iNOVA Capixaba, seja em sua unidade própria ou de suas filiais.

9.2 A Fundação iNOVA Capixaba no exercício de suas atribuições institucionais, desempenha funções inerentes à condição de controladora de dados pessoais, podendo também atuar como operadora desses dados, de forma direta ou por meio da contratação de pessoa jurídica.

9.3 São atribuições do controlador:

I – supervisionar o cumprimento desta Política, estabelecendo medidas para garantir a proteção de dados pessoais;

II – observar os fundamentos, princípios da privacidade e proteção de dados pessoais e os deveres impostos pela LGPD e por normativos correlatos no momento de decidir sobre tratamento ou de realizá-los;

III – elaborar o relatório de impacto à proteção de dados pessoais (RIPD);

IV – informar previamente o titular sobre as mudanças de finalidade para o tratamento de dados pessoais;

V – adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse;

VI – fornecer, sempre que solicitadas, informações adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos inerentes à atividade;

VII – indicar o encarregado pelo tratamento de dados pessoais no âmbito da Fundação iNOVA Capixaba;

VIII – comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, no prazo da legislação;

IX – manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado em legítimo interesse;

X – exercer outras funções impostas pela legislação vigente.

9.4 No atendimento ao disposto do item 9.3, inciso VIII, deverá ser informado, no mínimo:

- a. A descrição da natureza dos dados pessoais atingidos;
- b. As informações relativas aos titulares envolvidos;
- c. A especificação das medidas técnicas e administrativas de segurança adotadas para proteção dos dados;
- d. Os riscos decorrentes do incidente;
- e. As providências implementadas ou a serem adotadas para reverter ou mitigar os efeitos do evento.

9.5 São atribuições do operador:

- I – observar os princípios estabelecidos nesta Política, ao realizar o tratamento dos dados pessoais;
- II – realizar o tratamento de dados pessoais segundo as instruções fornecidas pelo controlador;
- III – manter o registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse; e
- IV – exercer outras funções impostas pela legislação vigente.

9.6 São atribuições do encarregado (DPO):

- I – receber e processar reclamações e comunicações dos titulares, além de prestar os esclarecimentos necessários e adotar medidas cabíveis;
- II – receber as comunicações da Autoridade Nacional de Proteção de Dados (ANPD) e promover as providências pertinentes;
- III – orientar os colaboradores da Fundação quanto às práticas e procedimentos a serem observados em matéria de proteção de dados pessoais;
- IV – coordenar internamente o fluxo de comunicação de incidentes, assegurando que o controlador realize as notificações legais nos prazos regulamentares; e
- V – desempenhar as demais atribuições fixadas em regulamentação complementar expedida pela ANPD;

9.7 Para o exercício de suas competências, o encarregado poderá requisitar apoio dos setores da Fundação iNOVA Capixaba, sendo-lhe assegurada a prerrogativa de reportar-se diretamente ao Diretor-Geral da Fundação iNOVA Capixaba e ao Conselho Curador.

9.8 A Fundação iNOVA Capixaba, no exercício de suas atividades como controladora de dados pessoais, responderá pelos danos patrimoniais, morais, individuais ou coletivos causados a titulares em decorrência do tratamento realizado em desconformidade com a legislação de proteção de dados ou da ocorrência de incidentes de segurança, nos termos dos arts. 42 a 45 da Lei nº 13.709/2018.

9.8.1 Verificado evento que caracterize tratamento inadequado ou incidente de segurança, a Fundação adotará as medidas necessárias à contenção dos efeitos e à proteção dos titulares afetados, sem prejuízo das obrigações de comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos próprios titulares, nos termos do item 9.4 desta Política.

9.8.2 A responsabilidade da Fundação somente poderá ser afastada nas hipóteses previstas no art. 43 da LGPD, quais sejam: (i) quando comprovado que não realizou o tratamento de dados pessoais que lhe é atribuído; (ii) quando, embora tenha realizado o tratamento, não houve violação à legislação de proteção de dados; ou (iii) quando o dano for decorrente de culpa exclusiva do titular ou de terceiros.

9.8.3 O operador que descumprir as instruções lícitas emanadas da Fundação na condição de controladora, ou que violar as obrigações decorrentes da legislação de proteção de dados, responderá solidariamente pelos danos causados ao titular, nos termos do art. 42, § 1º, da LGPD.

9.9 A identidade do Encarregado pelo tratamento de dados pessoais e seus canais de contato serão divulgados publicamente, de forma clara e objetiva, no sítio eletrônico oficial da Fundação iNOVA Capixaba.

9.9.1 Qualquer alteração na identidade ou nos canais de contato do Encarregado deverá ser refletida no sítio eletrônico da Fundação no prazo máximo de 5 (cinco) dias úteis contados da formalização da designação ou da respectiva alteração.

9.9.2 A divulgação de que trata este item deverá conter, no mínimo: (i) o nome completo ou a denominação do Encarregado; (ii) o endereço de correio eletrônico institucional destinado ao recebimento de comunicações de titulares e da ANPD; e (iii) demais canais de atendimento eventualmente disponibilizados pela Fundação para esse fim.

10 ESTRUTURA DE GOVERNANÇA DIGITAL E GESTÃO DA PROTEÇÃO DE DADOS

10.1 Será criada, na Fundação iNOVA Capixaba, a área de Governança Digital e Gestão da Proteção de Dados, responsável pela elaboração e atualização do Inventário de Dados Pessoais (IDP), que conterà o registro das operações de tratamento de dados pessoais pela Fundação.

10.2 A composição, a forma de atuação do setor, o conteúdo mínimo do IDP e os prazos para sua apresentação serão definidos em normativo interno próprio, devidamente aprovado pelo Diretor-Geral da Fundação.

11 RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

11.1 O Relatório de Impacto à Proteção de Dados Pessoais será elaborado pelo controlador, por intermédio de suas unidades organizacionais competentes, observadas as diretrizes:

I – a unidade responsável pelo projeto, processo ou atividade que envolva tratamento de dados pessoais deverá prestar as informações necessárias e subsidiar tecnicamente a elaboração do relatório, de modo a assegurar sua realização previamente ao início das operações de tratamento;

II – a coordenação da elaboração do relatório caberá ao setor de Governança Digital e Gestão da Proteção de Dados;

III – o encarregado atuará na orientação técnica, revisão e validação do relatório, bem como no atendimento às eventuais solicitações da ANPD;

IV – o relatório deverá ser submetido à aprovação da autoridade competente do controlador.

11.2 Será elaborado ou atualizado o RIPD sempre que houver potencial risco ou possibilidade de impacto relevante à privacidade e à proteção de dados pessoais, especialmente nas seguintes hipóteses:

I – implementação de nova tecnologia, sistema, serviço, programa, projeto ou qualquer iniciativa institucional que envolva o tratamento de dados pessoais e/ou dados pessoais sensíveis;

II – realização de monitoramento de localização de indivíduos ou qualquer modalidade de tratamento destinada à formação de perfil comportamental de pessoa natural identificada ou identificável;

III – tratamento de dados pessoais sensíveis;

IV – utilização de dados pessoais para a adoção de decisões automatizadas que produzam efeitos jurídicos ou impactos significativos sobre o titular, inclusive aquelas destinadas à definição de perfil pessoal, profissional, de consumo, de crédito ou aspectos da personalidade;

V – tratamento de dados pessoais de crianças e adolescentes, observadas as disposições específicas da LGPD;

VI – operações de tratamento que, em caso de incidente de segurança ou vazamento, possam acarretar danos patrimoniais, morais, individuais ou coletivos aos titulares dos dados;

VII – tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, quando aplicável à atuação institucional;

VIII – tratamento fundamentado no legítimo interesse do controlador;

IX – alterações na legislação e na regulamentação aplicáveis à proteção de dados e à privacidade, bem como modificações nas políticas institucionais, normas internas, sistema de informação, finalidades e bases legais do tratamento, meios técnicos utilizados, fluxos de dados novos ou modificados;

X – reestruturações administrativas que impliquem mudança na estrutura organizacional, com reflexos nos processos de tratamento de dados pessoais.

11.3 O Relatório de Impacto deverá conter, no mínimo, as seguintes informações:

11.3.1 Identificação dos Agentes de Tratamento:

- Identificação do controlador;
- Identificação do(s) operador(es), quando aplicável;
- Identificação do encarregado pelo tratamento de dados, com indicação dos canais de contato.

11.3.2 Deverá ser apresentada fundamentação clara acerca dos motivos que ensejaram a elaboração ou atualização do RIPD, indicando os fatores de risco identificados e sua relação com os direitos e garantias dos titulares.

11.3.3 O RIPD deverá demonstrar que o tratamento:

- Limita-se ao mínimo necessário para atingir sua finalidade;
- Observa os princípios da adequação e necessidade;
- Assegura mecanismos para garantia dos direitos previstos no art. 18 da LGPD;
- Adota salvaguardas contratuais quando houver operadores ou compartilhamento de dados;
- Implementa medidas de transparência e informação aos titulares.

11.3.4 O Relatório deverá conter análise estruturada dos riscos à privacidade, compreendendo:

- Descrição dos eventos de risco identificados;
- Avaliação da probabilidade de ocorrência;
- Análise do impacto potencial aos titulares;
- Classificação do nível de risco, conforme metodologia compatível com a Política de Gestão de Riscos da Fundação.

11.3.5 Deverão ser descritas as medidas técnicas e administrativas adotadas para mitigação dos riscos identificados, no que couber, tais como:

- Controles de acesso e autenticação;
- Criptografia e proteção de bases de dados;
- Registro e auditoria de acessos;
- Políticas de descarte seguro;
- Capacitação periódica de colaboradores;
- Cláusulas contratuais específicas com operadores e parceiros institucionais.

12 SANÇÕES E PENALIDADES

12.1 Sem prejuízo das sanções previstas na legislação vigente, a serem aplicadas pela autoridade competente, em caso de violação dos termos e procedimentos estabelecidos nesta política, deverão os administradores da Fundação tomar as medidas disciplinares cabíveis no âmbito interno da iNOVA Capixaba.

13 DISPOSIÇÕES FINAIS

13.1 A Fundação iNOVA Capixaba manterá o registro das operações de tratamento de dados pessoais que realizar, inclusive quanto à demonstração das razões e fundamentos para o tratamento quando embasado no legítimo interesse.

13.2 As disposições previstas nesta Política não excluem a aplicação de outras regras legais ou estatutárias não especificadas no texto.

