Siglas, definições e glossário:

PGPDP: Política Geral de Proteção de Dados Pessoais;

CGPDP: Comitê Gestor de Proteção de Dados;

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;

Autoridade Nacional de Proteção de Dados Pessoais: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais (LEI Nº 13.709, DE 14 DE AGOSTO DE 2018) em todo território nacional brasileiro;

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

Comitê Gestor de Proteção de Dados Pessoais: Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria do Hospital Nossa Senhora das Dores, que tem por finalidade tratar questões ligadas à Proteção de Dados Pessoais;

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

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

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

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

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

Segurança da informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações do Hospital Nossa Senhora das Dores;

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

Tratamento de dados pessoais: 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;

Usuário da informação: Empregados com vínculo empregatício de qualquer área das empresas que compõem o Hospital Nossa Senhora das Dores ou terceiros alocados na prestação de serviços ao Hospital Nossa Senhora das Dores, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizados a utilizar manipular qualquer ativo de informação do Hospital Nossa Senhora das Dores para o desempenho de suas atividades profissionais;

Violação de dados pessoais: situação em que dados pessoais são processados violando um ou mais requisitos relevantes de proteção da privacidade.

Objetivo

1. Esta política tem por propósito estabelecer diretrizes de Proteção de Dados que permitam ao Hospital Nossa Senhora das Dores realizar o tratamento de dados pessoais em conformidade com a legislação brasileira;

2. Orientar quanto à adoção de controles técnicos e administrativos para atendimento dos requisitos de Proteção de Dados Pessoais conforme a legislação vigente;

3. Resguardar os direitos fundamentais dos titulares dos dados, garantindo os seus direitos de liberdade e de privacidade;

4. Prevenir possíveis causas de violações de dados pessoais e incidentes de segurança da informação;

5. Minimizar os riscos ou de qualquer outro impacto negativo no negócio do Hospital Nossa Senhora das Dores.

Diretrizes

1. O objetivo da Proteção de Dados no Hospital Nossa Senhora das Dores é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à proteção de dados pessoais e dos direitos dos seus titulares, provendo suporte as operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos a organização.

2. A Provedoria, Diretoria Executiva e o Comitê Gestor de Proteção de Dados Pessoais estão comprometidos com uma gestão efetiva da Proteção de Dados Pessoais. Desta forma, adotam todas as medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação as necessidades do Hospital Nossa Senhora das Dores.

3. É política do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira:

I. Garantir ao titular a escolha de permitir ou não o tratamento dos seus dados pessoais, excetuando-se casos em que a lei aplicável permitir especificamente o processamento sem o seu consentimento;

II. Garantir que o objetivo do tratamento de dados pessoais esteja em conformidade com a legislação vigente e de acordo com uma base legal permitida;

III. Comunicar, de forma clara e adequadamente adaptada às circunstâncias, o tratamento de dados pessoais ao titular, antes do momento em que os dados são coletados ou usados pela primeira vez para um novo propósito;

IV. Sempre que necessário, fornecer ao titular explicações suficientes sobre o tratamento de seus dados pessoais, conforme previsto na legislação vigente;

V. Limitar a coleta de dados pessoais estritamente ao que é permitido e de acordo com a legislação vigente, minimizando, onde possível, a coleta dos dados pessoais;

VI. Limitar o uso, retenção, divulgação e transferência de dados pessoais ao necessário para cumprir com objetivos específicos, explícitos e legítimos;

VII. Reter dados pessoais apenas pelo tempo necessário para cumprir os propósitos declarados e, posteriormente, destruí-los, bloqueá-los ou anonimizá-los com segurança;

VIII. Bloquear o acesso a dados pessoais e não realizar mais nenhum tratamento quando os propósitos declarados expirarem, salvo, quando necessário para cumprimento de obrigação legal;

IX. Garantir a precisão e qualidade dos dados pessoais tratados, excetuando-se casos onde exista uma base legal para manter dados desatualizados;

X. Fornecer aos titulares dos dados pessoais, informações claras e facilmente acessíveis sobre as políticas, procedimentos e práticas com relação ao tratamento de dados pessoais realizado pela Instituição, incluindo quais dados são efetivamente tratados, a finalidade desse tratamento e informações sobre como entrar em contato para obter maiores detalhes;

XI. Notificar titulares quando ocorrerem alterações significativas no tratamento dos seus dados pessoais;

XII. Garantir que titulares tenham a possibilidade de acessar e revisar seus dados pessoais, desde que sua identidade seja autenticada com um nível apropriado de garantia, e que não exista nenhuma restrição legal a esse acesso ou a revisão dos dados pessoais.

XIII. Garantir a rastreabilidade e prestação de contas durante todo o tratamento de dados pessoais, incluindo quando dados pessoais forem compartilhados com terceiros;

XIV. Tratar integralmente violações de dados, garantindo que sejam adequadamente registradas, classificadas, investigadas, corrigidas e documentadas;

XV. Garantir que, na ocorrência de uma violação de dados, todas as partes interessadas serão notificadas, conforme requisitos e prazos previstos na legislação vigente.

XVI. Documentar e comunicar, conforme apropriado, todas as políticas, procedimentos e práticas relacionadas à privacidade e proteção de dados.

XVII. Garantir a existência de um responsável por documentar, implementar e comunicar políticas, procedimentos e práticas relacionadas à privacidade e proteção de dados;

XVIII. Adotar controles de segurança da informação, tanto técnicos quanto administrativos, suficientes para garantir níveis de proteção adequados para Dados Pessoais;

XIX. Disponibilizar políticas, normas e procedimentos de proteção de dados a todas as partes interessadas e autorizadas, tais como: colaboradores, terceiros contratados, onde for pertinente, e clientes;

XX. Garantir a educação e conscientização dos colaboradores, terceiros contratados, parceiros e clientes, sobre as práticas de proteção de dados pessoais adotadas pelo Hospital Nossa Senhora das Dores;

XXI. Melhorar continuamente a Gestão de Proteção de Dados Pessoais através da definição e revisão sistemática de objetivos de privacidade e proteção de dados pessoais em todos os níveis da organização;

XXII. Garantir a não discriminação no tratamento de dados pessoais;

XXIII. Garantir a conformidade integral com leis e regulamentações de proteção de Dados Pessoais.

Descrição

1. Comitê Gestor de Proteção de Dados Pessoais- CGPDP

I. Fica constituído o comitê gestor de proteção de dados pessoais, contando com a participação de, pelo menos, um representante da diretoria, e um membro das seguintes áreas: Tecnologia da Informação, Recursos Humanos, Jurídico, Marketing/Comunicação, e do Setor de Privacidade.

2. É responsabilidade do CGPDP:

I. Analisar, revisar e aprovar políticas e normas relacionadas à proteção de dados pessoais;

II. Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão da Proteção de Dados Pessoais;

III. Garantir que o tratamento de Dados Pessoais seja realizado em conformidade com a política geral de proteção de dados pessoais e demais legislações vigentes.

---

1. Encarregado pelo tratamento dos dados:

I. É responsabilidade do Encarregado pelo Tratamento de Dados Pessoais:

II. Aceitar reclamações e comunicações dos titulares de dados pessoais, prestar esclarecimentos e adotar as providências necessárias;

III. Receber comunicações da autoridade nacional de proteção de dados e adotar as providências necessárias;

IV. Orientar os colaboradores, terceiros contratados e demais partes do Hospital Nossa Senhora das Dores a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

V. Atender as demais atribuições, conforme orientação da Autoridade Nacional de Proteção de Dados, definidas em normas complementares publicadas pelo referido órgão;

VI. Atuar junto ao time de Segurança da Informação nos ajustes das normas e procedimentos de segurança da informação;

VII. Identificar e avaliar as principais ameaças à proteção de dados, bem como propor e, quando aprovado, apoiar a implantação de medidas corretivas para reduzir o risco;

VIII. Tomar as ações cabíveis para se fazer cumprir os termos desta política;

IX. Apoiar a gestão das violações de dados pessoais, garantindo tratamento adequado e comunicando, em prazo razoável, a autoridade nacional e titulares afetados pela violação sempre que esta representar risco ou dano relevante aos titulares.

---

1. Equipe de segurança da informação:

I. É responsabilidade do time de Segurança da Informação:

II. Garantir que políticas, normas e procedimentos de Segurança da Informação sejam ajustados de forma a atender os requisitos da Política Geral de Proteção de Dados Pessoais;

III. Adotar medidas de segurança, tanto técnicas quanto 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, conforme padrões mínimos recomendados pela autoridade nacional de proteção de dados pessoais;

IV. Realizar o tratamento de incidentes de segurança da informação que envolvam o tratamento de dados pessoais, garantindo sua detecção, contenção, eliminação e recuperação dentro de um prazo razoável;

V. Apoiar o Encarregado pelo tratamento de dados pessoais na comunicação à autoridade nacional e ao titular dos dados pessoais em casos de ocorrência de incidente de segurança que possam acarretar risco ou dano relevante aos titulares.

---

1. Usuários da Informação:

I. É responsabilidade dos Usuários da Informação:

II. Ler, compreender e cumprir integralmente os termos da Política Geral de Proteção de Dados Pessoais, bem como as demais normas e procedimentos de proteção de dados pessoais aplicáveis;

III. Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Proteção de Dados Pessoais, suas normas e procedimentos ao Encarregado pelo Tratamento de Dados Pessoais ou, quando pertinente, ao Comitê Gestor de Proteção de Dados Pessoais;

IV. Comunicar ao Encarregado pelo Tratamento de Dados Pessoais qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco Dados Pessoais tratados pelo Hospital Nossa Senhora das Dores;

V. Assinar o Termo de Uso de Sistemas de Informação, formalizando ciência e o aceite integral das disposições da Política Geral de Proteção de Dados Pessoais, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;

VI. Responder pela inobservância da Política Geral de Proteção de Dados Pessoais, normas e procedimentos relacionados ao tratamento de Dados Pessoais, conforme definido no item sanções e punições.

---

1. Sanções e Punições:

I. As violações, por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de proteção de dados pessoais, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e demissão por justa causa;

II. A aplicação de sanções e punições será realizada conforme a análise do Comitê Gestor de Proteção de Dados Pessoais, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o comitê, no uso do seu poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

III. No caso de terceiros contratados ou prestadores de serviço, o comitê deverá analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato;

IV. Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em riscos aos titulares de dados pessoais, ou dano ao Hospital Nossa Senhora das Dores, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes, sem prejuízo aos termos descritos nos itens I,II, e III desse tópico.

1. Casos Omissos:

I. Os casos omissos serão avaliados pelo Comitê Gestor de Proteção de Dados Pessoais para posterior deliberação.

2. As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de proteção de dados pessoais, não se esgotam em razão da contínua evolução tecnológica, da legislação vigente e constante surgimento de novas ameaças e requisitos. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção de dados pessoais tratados pelo Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira.

Referências

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Indicadores de Efetividade

Auditorias em prontuários médicos; e

Incidente de segurança

Controle Histórico				
Revisão	**Data**	**Elaboração / Revisão**	**Verificação**	**Aprovação**
1	04/04/2025	Gustavo N.V. Rocha	Welisson Geraldo D. Reis	Juliana A. B. Silva Souza

Controle De Revisão			
Revisão	**Data**	**Item**	**Natureza das Alterações**
1	04/04/2025	NA	NA