

INSTITUTO MEMORIAL DO AGRESTE

Política de Proteção de Dados Pessoais

Programa de Integridade · Edição 2026
Versão 01 — Política Institucional

DOCUMENTO

Política de Proteção de Dados Pessoais
Código HMP.POL.010

UNIDADE HOSPITALAR

Hospital Memorial de Pernambuco - HMP
IMA - Instituto Memorial do Agreste - CNPJ 24.262.537/0001-98

CARUARU - PERNAMBUCO

Edição Institucional · 2026

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS
HOSPITAL MEMORIAL DE PERNAMBUCO – HMP

Objeto

Esta Política estabelece diretrizes, responsabilidades e controles para orientar o tratamento e a proteção de dados pessoais no âmbito do Hospital Memorial de Pernambuco – HMP, em conformidade com a Lei Geral de Proteção de Dados Pessoais – LGPD.

O documento integra o Programa de Integridade do HMP e busca assegurar que dados de pacientes, acompanhantes, colaboradores, corpo clínico, fornecedores, prestadores de serviço e demais titulares sejam tratados com finalidade legítima, segurança, confidencialidade e transparência.

Ficha Técnica

Documento	Política de Proteção de Dados Pessoais
Código	HMP.POL.010
Versão	01
Edição	2026
Classificação	Pública
Mantenedora	IMA – Instituto Memorial do Agreste · CNPJ 24.262.537/0001-98
Unidade	Hospital Memorial de Pernambuco – HMP · CNES 4222466
Abrangência	Todas as unidades, colaboradores, corpo clínico, terceiros, operadores, fornecedores, prestadores de serviço, representantes e parceiros
Base legal	Lei nº 13.709/2018 – LGPD; Lei nº 13.853/2019; Constituição Federal; normas e orientações da ANPD; legislação sanitária, trabalhista, contratual, assistencial e demais normas aplicáveis
Vigência / Revisão	Bienal, ou antes, diante de alteração normativa, incidente relevante, mudança de sistema ou necessidade institucional

Elaborador	Aline Melissa Santos Oliveira	Resp. Área de Integridade	26/08/2026
Revisor	Flaviano Neves de Andrade	Diretor Administrativo	26/08/2026
Aprovador	Sidney Souza Araújo Ribeiro	Diretor Presidente	28/09/2026

Sumário

1. Propósito e campo de aplicação
2. Público abrangido e dever de cumprimento
3. Bases legais e documentos complementares
4. Definições práticas
5. Diretrizes de privacidade e proteção de dados
6. Tratamento de dados de saúde e dados sensíveis
7. Direitos dos titulares e canais de atendimento
8. Segurança da informação, sigilo e controle de acesso
9. Compartilhamento, terceiros e operadores
10. Incidentes de segurança e resposta institucional
11. Registros, retenção e descarte de dados
12. Responsabilidades, capacitação, monitoramento e revisão

1. Propósito e campo de aplicação

Esta Política define parâmetros para que o HMP realize o tratamento de dados pessoais e dados pessoais sensíveis com segurança, finalidade legítima, transparência e alinhamento ao Programa de Integridade.

Seu propósito é orientar a coleta, o acesso, o uso, o armazenamento, o compartilhamento, a retenção, o descarte e a proteção de informações pessoais tratadas em meio físico ou digital.

O cumprimento destas regras busca reduzir riscos de exposição indevida de dados, acesso sem autorização, uso excessivo de informações, falhas de sigilo, incidentes de segurança e descumprimento da LGPD.

2. Público abrangido e dever de cumprimento

Esta Política se aplica à Alta Administração, conselhos, diretoria, gestores, lideranças, corpo clínico, colaboradores, residentes, estagiários, aprendizes, voluntários, fornecedores, prestadores de serviço, consultores, representantes, operadores, parceiros e demais pessoas que tratem dados pessoais relacionados ao HMP.

As orientações devem ser observadas por todos que coletem, registrem, consultem, alterem, imprimam, transmitam, compartilhem, arquivem ou eliminem dados pessoais no exercício de atividades institucionais.

Terceiros e prestadores deverão respeitar as normas internas do HMP, as cláusulas contratuais, o Código de Conduta para Fornecedores e Representantes, as regras de sigilo, proteção de dados, segurança da informação, biossegurança e conduta profissional.

3. Bases legais e documentos complementares

Esta Política deve ser interpretada em conjunto com o Código de Ética e Conduta, a Política Antifraude e Anticorrupção, a Política de Canal de Denúncias, Apuração e Não

Retaliação, a Política de Compras, Contratações e Gestão de Terceiros, a Política de Governança Corporativa, a Política de Gestão de Riscos e demais normativos do HMP.

São referências para sua aplicação a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais, a Lei nº 13.853/2019, normas e orientações da Autoridade Nacional de Proteção de Dados, legislação sanitária, trabalhista, contratual, profissional, arquivística e demais obrigações aplicáveis.

Nenhuma orientação verbal, prática informal, urgência operacional, interesse administrativo ou solicitação de terceiros poderá afastar a necessidade de finalidade, necessidade, segurança, confidencialidade, registro adequado e respeito aos direitos dos titulares.

4. Definições práticas

Dado pessoal é qualquer informação relacionada a pessoa natural identificada ou identificável, incluindo nome, documento, contato, endereço, imagem, voz, matrícula, dados profissionais, dados cadastrais e informações de atendimento.

Dado pessoal sensível é a informação sobre saúde, dado genético ou biométrico, origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, vida sexual ou outra informação que exija proteção reforçada pela legislação.

Tratamento é toda operação realizada com dados pessoais, como coleta, acesso, registro, organização, consulta, uso, compartilhamento, transmissão, arquivamento, eliminação, modificação, classificação ou armazenamento.

Titular é a pessoa natural a quem os dados se referem. Controlador é quem decide sobre o tratamento. Operador é quem trata dados em nome do controlador. Encarregado é o canal de comunicação com titulares e com a Autoridade Nacional de Proteção de Dados, quando designado.

5. Diretrizes de privacidade e proteção de dados

O tratamento de dados no HMP deverá observar finalidade, adequação, necessidade, transparência, qualidade dos dados, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

As áreas devem utilizar apenas os dados necessários ao desempenho de suas atribuições, evitando coleta excessiva, cópias desnecessárias, impressão sem justificativa, circulação indevida de documentos e armazenamento em canais não autorizados.

A proteção de dados deve ser considerada em processos assistenciais, administrativos, trabalhistas, financeiros, contratuais, acadêmicos, tecnológicos, de prestação de contas, de comunicação institucional e de relacionamento com órgãos públicos e privados.

6. Tratamento de dados de saúde e dados sensíveis

O HMP trata dados pessoais sensíveis principalmente para prestação de serviços de saúde, execução de obrigações legais e regulatórias, proteção da vida, tutela da saúde, gestão assistencial, relação de trabalho, faturamento, auditoria e execução de contratos.

Dados de prontuário, exames, prescrições, diagnósticos, evoluções, imagens, dados biométricos, informações trabalhistas e registros de atendimento deverão ser acessados somente por pessoas autorizadas e para finalidade compatível com sua função.

Em caso de dúvida sobre base legal, necessidade do dado, legitimidade do acesso ou forma de compartilhamento, a liderança ou área responsável deverá ser consultada antes da continuidade do tratamento.

7. Direitos dos titulares e canais de atendimento

O HMP deverá observar os direitos dos titulares previstos na LGPD, incluindo confirmação de tratamento, acesso, correção, informações sobre compartilhamentos, revisão quando aplicável, anonimização, bloqueio ou eliminação nas hipóteses legais cabíveis.

Solicitações de titulares deverão ser recebidas por canal institucional, registradas, avaliadas e respondidas de forma segura, observadas a identidade do solicitante, o sigilo

profissional, a guarda obrigatória de documentos, a segurança do paciente e os limites legais aplicáveis.

Informações pessoais não deverão ser fornecidas a terceiros sem fundamento legal, autorização adequada, comprovação de legitimidade ou validação da área competente, especialmente quando envolver dados de saúde, crianças, adolescentes, trabalhadores ou pessoas vulneráveis.

8. Segurança da informação, sigilo e controle de acesso

O acesso a dados pessoais deverá ser limitado às pessoas autorizadas e necessárias à atividade, mediante credenciais individuais, senhas protegidas, perfis adequados e uso de sistemas ou meios institucionais aprovados.

É vedado compartilhar senhas, usar login de outra pessoa, acessar prontuários por curiosidade, enviar dados por canais pessoais sem autorização, divulgar imagens de pacientes ou colaboradores sem permissão ou discutir casos em ambientes públicos.

Documentos físicos, relatórios, prontuários, formulários, arquivos digitais, dispositivos, e-mails e sistemas deverão ser mantidos sob controle adequado, com atenção ao armazenamento, transporte, impressão, descarte, acesso e confidencialidade.

9. Compartilhamento, terceiros e operadores

O compartilhamento de dados com fornecedores, laboratórios, operadoras, auditores, órgãos públicos, profissionais de saúde, parceiros ou prestadores deverá observar finalidade legítima, necessidade, segurança, confidencialidade, registro e instrumento jurídico adequado.

A contratação de terceiros que tratem dados pessoais em nome do HMP deverá considerar a natureza dos dados, volume de informações, acesso a sistemas, criticidade assistencial, medidas de segurança, histórico de conformidade e capacidade de cumprir a LGPD.

Sempre que aplicável, contratos e instrumentos relacionados deverão prever confidencialidade, proteção de dados, finalidade do tratamento, medidas de segurança, restrição de subcontratação, comunicação de incidentes, cooperação com auditorias e devolução ou eliminação de dados ao término da relação.

10. Incidentes de segurança e resposta institucional

Qualquer suspeita de vazamento, perda, extravio, acesso indevido, envio equivocado, exposição de prontuário, invasão de sistema, compartilhamento inadequado ou uso não autorizado de dados pessoais deverá ser comunicada imediatamente à liderança ou à área responsável.

A resposta institucional deverá avaliar natureza dos dados, quantidade de titulares, riscos envolvidos, medidas de contenção, preservação de evidências, necessidade de comunicação ao titular, à autoridade competente ou a outras instâncias, conforme legislação e orientação interna.

É proibido ocultar incidente conhecido, apagar evidências, retardar comunicação interna, responsabilizar indevidamente quem comunicou situação de boa-fé ou tratar ocorrências de proteção de dados sem observância dos fluxos institucionais.

11. Registros, retenção e descarte de dados

O HMP deverá manter documentos e registros pelo prazo necessário ao cumprimento de finalidades assistenciais, legais, regulatórias, contratuais, trabalhistas, fiscais, de auditoria, defesa de direitos e prestação de contas.

O descarte de documentos físicos ou digitais contendo dados pessoais deverá ocorrer de forma segura, controlada e compatível com a natureza da informação, evitando exposição, reutilização indevida, perda de rastreabilidade ou eliminação de documento que ainda possua obrigação de guarda.

Registros de acesso, logs, termos, contratos, respostas a titulares, comunicações de incidentes, evidências de treinamento e demais documentos de conformidade poderão ser preservados como prova de responsabilização e prestação de contas.

12. Responsabilidades, capacitação, monitoramento e revisão

As lideranças devem orientar suas equipes, assegurar acessos proporcionais às funções, comunicar riscos, restringir circulação de informações sensíveis, preservar documentos e aplicar esta Política em suas rotinas.

A área de Integridade, o Encarregado de Dados, quando designado, Tecnologia da Informação, Jurídico, Recursos Humanos, Qualidade, Segurança do Paciente e demais áreas responsáveis poderão atuar em conjunto na orientação, capacitação, análise de riscos, resposta a incidentes e melhoria dos controles.

Esta Política deverá ser divulgada aos públicos abrangidos, aplicada em treinamentos e revisada a cada dois anos ou antes, quando houver alteração normativa, orientação da ANPD, mudança de sistema, incidente relevante ou necessidade de aperfeiçoamento institucional.