RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

(RIPD / DPIA)

HUB HEALTH DISTRIBUIDORA DE PRODUTOS HOSPITALARES LTDA.

2026

Versão 2.0 — Atualização legislativa e técnica
(substitui a Versão 1.0, de 01/08/2025)

EMPRESA: HUB HEALTH DISTRIBUIDORA DE PRODUTOS HOSPITALARES LTDA., pessoa jurídica de direito privado inscrita no CNPJ sob o nº 42.705.829/0001-30, com sede na Rodovia BR-116, nº 2.555, Módulo 5, Fortaleza/CE, CEP 60.824-115. Neste ato, representada por seu representante legal **MARIO KANASHIRO FILHO**, portador da Cédula de Identidade RG nº 20.695.261-2 SSP/SP, inscrito no CPF sob o nº 164.285.718-11, residente e domiciliado no Estado de São Paulo.

RESPONSÁVEL PELO TRATAMENTO / DPO (ENCARREGADO): Luciana Alves Campos, advogada inscrita na OAB/SP sob o nº 186.345.

CANAL DE ATENDIMENTO DO ENCARREGADO: luciana.juridico@hubhealthmed.com.br

COMUNICAÇÃO DA INDICAÇÃO DO ENCARREGADO (Resolução CD/ANPD nº 2/2022): Registro Interno realizado em 01 de agosto de 2025.

ÁREA RESPONSÁVEL PELA ELABORAÇÃO: Jurídico e Compliance

Fortaleza/CE, 01 de agosto de 2026.
Versão 2.0

0. Controle de Versões

Este documento substitui integralmente a Versão 1.0 (01/08/2025). As alterações têm por objetivo refletir o amadurecimento do programa de privacidade da Hub Health e as atualizações normativas editadas pela Autoridade Nacional de Proteção de Dados (ANPD) desde a emissão da versão anterior, tornando a análise mais técnica, granular e auditável.

Versão	Data	Descrição da alteração	Responsável
1.0	01/08/2025	Emissão inicial do RIPD.	Jurídico e Compliance
2.0	01/08/2026	Emissão da Versão 2.0 para a Hub Health, incorporando: (I) as atualizações técnicas e legislativas realizadas para o grupo — revisão das bases legais à luz dos incisos do art. 7º da LGPD; inclusão de módulo de transferência internacional (Resolução CD/ANPD nº 19/2024); inclusão de protocolo de gestão de incidentes (Resolução CD/ANPD nº 15/2024); atualização da metodologia de risco (ISO/IEC 29134 e ISO/IEC 27005:2022); expansão da matriz de riscos, do plano de tratamento e das cláusulas de due diligence de terceiros; e (II) as correções decorrentes de análise jurídica de auditoria interna — padronização e correção da metodologia de cálculo de risco (soma P+I, com reclassificação dos riscos 5, 6 e 7); formalização do teste de legítimo interesse (LIA, Anexo II); inclusão de campo de controle da comunicação da indicação do DPO à ANPD; antecipação de 180 para 90 dias do prazo de formalização de salvaguardas de transferência internacional; correção da referência ao art. 39 da LGPD para os arts. 46 a 48; referência ao ROPA (Anexo III); mapeamento de rastreabilidade sanitária (ANVISA); canal adicional de atendimento a titulares; e princípio de Privacy by Design/by Default (Seção 14).	Jurídico e Compliance

1. Introdução, Objetivo e Base Normativa para Elaboração do RIPD

O presente Relatório de Impacto à Proteção de Dados Pessoais ("RIPD") é elaborado pela Hub Health Distribuidora de Produtos Hospitalares Ltda. ("Hub Health" ou "Companhia") em atendimento aos artigos 5º, XVII, e 38 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - "LGPD"), que facultam à Autoridade Nacional de Proteção de Dados ("ANPD") a exigência de relatório específico sobre operações de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais, bem como aos princípios da prevenção (art. 6º, VIII) e da responsabilização e prestação de contas - accountability (art. 6º, X e art. 50, §2º, I, "b") da LGPD.

O documento tem por finalidade: (i) descrever de forma estruturada o ciclo de vida do tratamento de dados pessoais de clientes, potenciais clientes e representantes comerciais; (ii) identificar as bases legais aplicáveis a cada finalidade; (iii) mapear os riscos à privacidade e à segurança da informação associados ao tratamento; e (iv) evidenciar as medidas técnicas, administrativas e organizacionais adotadas para mitigar tais riscos a um nível residual aceitável, permitindo a demonstração de conformidade (accountability) perante a ANPD, parceiros contratuais e órgãos públicos contratantes.

1.1. Referencial normativo e técnico considerado

- Lei nº 13.709/2018 (LGPD) e alterações posteriores;
- Lei nº 12.965/2014 (Marco Civil da Internet) e Decreto nº 8.771/2016, no que se refere à guarda de registros e à segurança de dados;
- Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023 — Regulamento de Dosimetria e Aplicação de Sanções Administrativas previstas na LGPD;
- Resolução CD/ANPD nº 15, de 2024 — Regulamento de Comunicação de Incidentes de Segurança que possam acarretar risco ou dano relevante aos titulares;
- Resolução CD/ANPD nº 19, de 2024 — Regulamento de Transferência Internacional de Dados Pessoais, cláusulas-padrão contratuais e hipóteses de dispensa;
- Guias orientativos da ANPD sobre tratamento de dados pessoais pela administração pública, definições de agentes de tratamento e elaboração de relatórios de impacto;
- ABNT NBR ISO/IEC 29134:2017 — Diretrizes para avaliação de impacto à privacidade;
- ABNT NBR ISO/IEC 27005:2022 — Gestão de riscos de segurança da informação;
- ABNT NBR ISO/IEC 27701:2019 — Sistema de gestão de informações de privacidade (referência complementar);
- Lei nº 14.133/2021 (Nova Lei de Licitações), quanto às finalidades de tratamento decorrentes de contratos administrativos celebrados com entes públicos, atividade central do Grupo.

2. Identificação do Tratamento Avaliado

Título do Tratamento: Cadastro e Gestão de Clientes para Fins de Faturamento, Entrega de Produtos e Comunicação Institucional.

Natureza da atividade: distribuição atacadista de medicamentos e produtos hospitalares, com atuação relevante em contratações públicas.

Setores envolvidos diretamente no tratamento: Comercial, Financeiro, Licitação, Logística, Tecnologia da Informação (TI), Compras e Jurídico/Compliance.

Sistemas e ativos de informação envolvidos: ERP TOTVS (módulo de gestão comercial, financeiro e fiscal), formulários eletrônicos do sítio institucional, sistema de CRM para histórico de relacionamento comercial, ambiente de correio eletrônico corporativo e portais de licitação/compras governamentais (ComprasNet, SEI/SP, e demais plataformas de pregão eletrônico).

Descrição do Processo: o tratamento tem início com a coleta de dados pessoais e comerciais de clientes (pessoas jurídicas, seus representantes) e de potenciais clientes, inclusive órgãos públicos, no contexto de propostas comerciais e processos licitatórios. Os dados são inseridos e centralizados no sistema de gestão empresarial (ERP TOTVS), que integra as áreas comercial, financeira e logística, permitindo o acompanhamento de toda a jornada contratual - da proposta ao faturamento e entrega. Após a coleta, os dados são armazenados em bases de dados corporativas segregadas por ambiente de produção, homologação e backup, sujeitas a controles de acesso baseados em perfis funcionais.

Parágrafo primeiro: além do uso interno, os dados coletados e armazenados podem ser compartilhados com parceiros logísticos (transportadoras), para fins de entrega dos produtos adquiridos; com a contabilidade terceirizada e auditores, para fins de apuração e conformidade fiscal e financeira; com instituições financeiras e plataformas de pagamento, para a efetivação das transações; e, quando aplicável, com órgãos da Administração Pública contratante, no âmbito da execução e fiscalização contratual, sempre com base no cumprimento de requisitos legais, regulatórios ou contratuais.

Parágrafo segundo: a utilização e o compartilhamento de dados são realizados de forma controlada e conforme as finalidades previamente informadas aos titulares, observando os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas, previstos no art. 6º da LGPD.

3. Metodologia de Avaliação

A presente avaliação de impacto adota metodologia híbrida, combinando os critérios qualitativos recomendados pela ABNT NBR ISO/IEC 29134:2017 para identificação e priorização de riscos à privacidade, com a estrutura de gestão de riscos de segurança da informação da ABNT NBR ISO/IEC 27005:2022 para a classificação de probabilidade e impacto. O processo compreendeu: (i) mapeamento do fluxo de dados e dos ativos envolvidos; (ii) identificação de ameaças e vulnerabilidades associadas a cada etapa do ciclo de vida do dado; (iii) estimativa de probabilidade e impacto por meio de matriz de risco; (iv) definição de controles de mitigação já implementados e de controles adicionais recomendados; e (v) apuração do risco residual, com validação pelo Encarregado (DPO) e pela área de Jurídico e Compliance.

3.1. Critérios de classificação de probabilidade e impacto

Nível	Probabilidade (ocorrência)	Impacto (severidade ao titular/à Companhia)
Baixo - pontuação 5	Evento improvável; não há histórico de ocorrência nos últimos 24 meses e os controles existentes reduzem significativamente a chance de materialização.	Impacto limitado, reversível e de curta duração; sem exposição de dados sensíveis ou financeiros relevantes.

Nível	Probabilidade (ocorrência)	Impacto (severidade ao titular/à Companhia)
Moderado - pontuação 15	Evento possível; pode ocorrer eventualmente, com histórico esporádico no setor ou indícios de vulnerabilidade não totalmente sanada.	Impacto relevante, mas circunscrito a um grupo limitado de titulares, com efeitos reversíveis mediante ação corretiva tempestiva.
Alto - pontuação 30	Evento provável; existe histórico recorrente no setor, ausência de controle compensatório ou exposição de superfície de ataque relevante.	Impacto severo, potencialmente irreversível, com exposição de dados em volume relevante, dano à reputação, a direitos fundamentais dos titulares ou sanção regulatória significativa.

O nível de risco é apurado pela soma Probabilidade + Impacto (P + I), ambos pontuados exclusivamente na escala fixa de 5 (Baixo), 15 (Moderado) ou 30 (Alto) definida na tabela acima. Essa escala fixa produz seis resultados possíveis — 10, 20, 30, 35, 45 e 60 —, classificados de forma exaustiva na Tabela de Classificação de Risco (Seção 12), sem lacunas entre faixas.

4. Mapeamento do Fluxo de Dados (Ciclo de Vida)

O quadro a seguir consolida, de forma técnica, a origem, a categoria de dado, o sistema utilizado, a finalidade, a base legal aplicável e o prazo de retenção associados a cada etapa relevante do tratamento, permitindo rastreabilidade integral do dado pessoal ao longo de seu ciclo de vida na Companhia.

Origem	Categoria de dado	Sistema/Ativo	Finalidade	Base legal (art. 7º LGPD)	Retenção
Processo licitatório (edital, proposta, habilitação)	Razão social, CNPJ, dados do representante legal, documentos de habilitação	ERP TOTVS / portais de licitação	Participação em certame e execução contratual	II — Cumprimento de obrigação legal/regulatória; V — Execução de contrato	Prazo contratual + prazo prescricional aplicável (mín. 5 anos, Lei nº 14.133/2021)
Atendimento comercial (telefone/e-mail)	Nome, cargo, contato do representante	CRM / ERP TOTVS	Atendimento e pós-venda	V — Execução de contrato; IX — Legítimo interesse	Até 5 anos após o último contato
Faturamento e cobrança	Razão social, CNPJ, dados bancários, endereço de cobrança	ERP TOTVS (módulo financeiro)	Emissão de nota fiscal, cobrança e conciliação financeira	II — Cumprimento de obrigação legal (fiscal); V — Execução de contrato	5 anos (prazo decadencial/prescricional tributário, art. 173 e 174 do CTN)
Logística/expedição	Nome do destinatário, endereço de entrega, telefone	ERP TOTVS / sistemas de transportadoras parceiras	Entrega dos produtos adquiridos	V — Execução de contrato	Até 5 anos após o último contato
Comunicação institucional/marketing	Nome, e-mail, telefone	CRM / ferramenta de e-mail marketing	Envio de comunicações institucionais ou promocionais	I — Consentimento do titular	Até a revogação do consentimento ou 5 anos de inatividade
Rastreabilidade sanitária da cadeia farmacêutica	Nome, cargo e contato de representantes/profissionais de saúde envolvidos na cadeia de distribuição	ERP TOTVS / sistemas de controle sanitário	Cumprimento das exigências de rastreabilidade da ANVISA (RDC nº 204/2017 e legislação sanitária correlata)	II — Cumprimento de obrigação legal/regulatória	Prazo mínimo exigido pela legislação sanitária aplicável (não inferior a 5 anos)

As fontes de coleta permanecem as identificadas na versão anterior deste RIPD, armazenadas em servidores/ambientes de nuvem corporativos segregados por perfil de acesso, com eliminação segura e irreversível ao término do prazo de retenção aplicável, ressalvada a hipótese de obrigação legal que imponha prazo superior.

5. Finalidade do Tratamento

1. Execução de contratos de venda e fornecimento, inclusive os decorrentes de processos licitatórios regidos pela Lei nº 14.133/2021 e, residualmente, pela Lei nº 8.666/1993;
2. Faturamento, cobrança e entrega de pedidos;
3. Atendimento ao cliente e relacionamento pós-venda;
4. Envio de comunicações institucionais ou promocionais, sempre mediante consentimento específico e destacado do titular;
5. Cumprimento de obrigações fiscais, contábeis, regulatórias (inclusive perante a ANVISA e Vigilâncias Sanitárias) e de fiscalização contratual perante entes públicos contratantes;
6. Prevenção à fraude e à inadimplência, e defesa em processos administrativos e judiciais decorrentes da relação contratual.

6. Bases Legais Aplicáveis, conforme a Lei Geral de Proteção de Dados

Diferentemente da versão anterior, que citava isoladamente o art. 10 da LGPD como base legal autônoma para o legítimo interesse, esta atualização corrige e detalha o enquadramento técnico correto: o legítimo interesse é hipótese autorizativa prevista no art. 7º, inciso IX, da LGPD, sendo o art. 10 o dispositivo que disciplina seus limites e o dever de realização de teste de proporcionalidade pelo controlador. A tabela a seguir consolida o mapeamento finalidade × base legal:

Base legal (art. 7º, LGPD)	Descrição	Aplicação no tratamento avaliado
I — Consentimento	Manifestação livre, informada e inequívoca do titular quanto a finalidade determinada.	Envio de comunicações institucionais e promocionais, sempre revogável a qualquer tempo pelo titular, nos termos do art. 8º, §5º, da LGPD.
II — Cumprimento de obrigação legal ou regulatória	Tratamento necessário para atendimento de obrigação imposta ao controlador por lei ou regulação.	Emissão de documentos fiscais, retenção de registros contábeis/tributários e cumprimento de exigências sanitárias (ANVISA) aplicáveis à distribuição de medicamentos.
V — Execução de contrato ou de procedimentos preliminares	Tratamento necessário à execução de contrato do qual o titular seja parte, ou de diligências pré-contratuais a seu pedido.	Gestão da relação comercial, faturamento, logística e cumprimento de obrigações contratuais com clientes privados e públicos.
IX c/c art. 10 — Legítimo interesse do controlador	Tratamento fundamentado em finalidades legítimas, consideradas a partir de situações concretas, respeitadas as expectativas do titular e seus direitos e liberdades fundamentais.	Prospecção comercial (leads), atendimento pós-venda, prevenção a fraudes e análise de satisfação, sempre acompanhados de teste de balanceamento ("legitimate interest assessment") e registro documental, conforme art. 10, §2º, da LGPD.
Bases específicas de licitações públicas	Tratamento de dados de representantes de órgãos públicos e de agentes públicos no bojo de processos licitatórios.	Aplicação combinada dos incisos II e V do art. 7º da LGPD com a Lei nº 14.133/2021 (ou Lei nº 8.666/1993, conforme a modalidade e vigência contratual), que impõem o tratamento de dados de habilitação e de representação legal como condição de participação no certame.

O tratamento fundamentado no legítimo interesse (art. 7º, IX c/c art. 10 da LGPD) é acompanhado de teste de proporcionalidade - Legitimate Interest Assessment (LIA) -, formalizado como documento autônomo mantido pela área de Jurídico e Compliance e sintetizado neste RIPD no Anexo II, em atendimento ao dever de transparência do art. 10, §2º, da LGPD.

Não há, no tratamento ora avaliado, hipótese de tratamento de dados pessoais sensíveis (art. 5º, II, da LGPD) em caráter estrutural. Eventual dado incidental de saúde de representante comercial (ex.: informação voluntária em atendimento) não integra finalidade do tratamento e, caso ocorra, deve ser expurgado do registro conforme procedimento de minimização de dados.

6.1. Registro das Operações de Tratamento (ROPA)

O inventário completo de todas as atividades de tratamento de dados pessoais realizadas pela Companhia — não apenas a atividade específica avaliada neste RIPD — consta do Registro das Operações de Tratamento de Dados Pessoais (ROPA), documento autônomo mantido e atualizado pela área de Jurídico e Compliance em conjunto com o Encarregado, em atendimento ao art. 37 da LGPD. O ROPA é referenciado neste RIPD como Anexo III e deve ser consultado para a visão consolidada de todas as demais atividades de tratamento da Partner Farma, da Átons do Brasil e da Hub Health.

7. Categorias de Titulares

- Clientes (pessoas jurídicas, seus representantes legais e prepostos);
- Órgãos e entidades da Administração Pública, na qualidade de contratantes, e respectivos agentes públicos representantes;
- Potenciais clientes (leads comerciais e participantes de processos licitatórios);
- Representantes comerciais e prepostos de fornecedores/parceiros logísticos, quando aplicável.

8. Categorias de Dados Pessoais Tratados

- Nome completo / Razão social e nome fantasia;
- CPF / CNPJ e Inscrição Estadual;
- E-mail, telefone e endereço comercial ou de entrega;
- Dados bancários, em hipóteses específicas de faturamento e conciliação financeira;
- Histórico de compras, propostas e interações comerciais;
- Dados de representação legal e documentos de habilitação exigidos em processos licitatórios (procurações, certidões, atos constitutivos).

Não são tratados, no âmbito deste processo, dados pessoais sensíveis na acepção do art. 5º, II, da LGPD *(origem racial ou étnica, convicção religiosa, opinião política, dado referente à saúde ou à vida sexual, dado genético ou biométrico),* tampouco dados de crianças e adolescentes, o que reduz o grau de criticidade do tratamento sob a ótica do art. 14 da LGPD.

9. Compartilhamento e Transferência de Dados

9.1. Compartilhamento nacional

Os dados pessoais tratados pela Hub Health podem ser compartilhados com os agentes indicados na tabela a seguir, todos vinculados por instrumento contratual com cláusulas específicas de proteção de dados pessoais, obrigações de confidencialidade e, quando aplicável, sub-rogação de responsabilidade em caso de incidente de segurança causado pelo operador.

Destinatário	Natureza	País/Região	Fundamento
Transportadoras parceiras	Operador de dados	Brasil	Execução de contrato (art. 7º, V) e contrato com cláusulas de proteção de dados
Escritório de contabilidade terceirizado	Operador de dados	Brasil	Cumprimento de obrigação legal (art. 7º, II)
Fabricantes/laboratórios (Sandoz, EMS, Accord, Dr. Reddy's e demais)	Controlador/operador conforme o caso, para fins de comprovação de desabastecimento e regularidade sanitária	Predominantemente Brasil, com matrizes/plantas no exterior	Execução de contrato e cumprimento de obrigação regulatória; eventual transferência internacional avaliada conforme Seção 10.1
Plataformas de pagamento e instituições financeiras	Operador de dados	Brasil	Execução de contrato (art. 7º, V)

9.2. Transferência internacional de dados pessoais

A Companhia mantém relacionamento comercial com fabricantes e distribuidores multinacionais de insumos farmacêuticos, cujas matrizes podem estar sediadas fora do território nacional. Sempre que o tratamento envolver o efetivo envio de dados pessoais *(nomes e contatos de representantes, por exemplo)* a destinatário localizado no exterior, a operação deverá observar o Regulamento de Transferência Internacional de Dados Pessoais aprovado pela ANPD (Resolução CD/ANPD nº 19/2024), que prevê como hipóteses aptas a legitimar a transferência, entre outras: (i) decisão de adequação do país ou organismo internacional de destino; (ii) garantias específicas prestadas pelo controlador, tais como cláusulas-padrão contratuais publicadas pela ANPD, cláusulas contratuais específicas, normas corporativas globais ou selos e certificados; e (iii) hipóteses legais específicas do art. 33 da LGPD.

10. Direitos dos Titulares e Procedimento de Atendimento

A Hub Health disponibiliza aos titulares canal direto de comunicação com o Encarregado (DPO) para exercício dos direitos previstos no art. 18 da LGPD. As solicitações são registradas, triadas pela área de Jurídico e Compliance e respondidas dentro dos prazos internos de referência abaixo, observadas eventuais prorrogações devidamente justificadas e comunicadas ao titular.

Considerando o perfil dos titulares - clientes localizados em diferentes regiões do país, inclusive órgãos públicos sem acesso facilitado ao e-mail corporativo -, a Companhia disponibiliza, além do canal eletrônico principal, um canal adicional de atendimento por meio de formulário eletrônico disponível no sítio institucional e/ou telefone (*PABX (15) 3217-1038*), em linha com o Guia Orientativo sobre Direitos dos Titulares da ANPD.

Direito do titular (art. 18, LGPD)	Prazo de resposta interno	Canal
Confirmação da existência de tratamento e acesso aos dados	Até 15 dias corridos, conforme prazo de referência da ANPD para resposta simplificada, prorrogável mediante justificativa	luciana.juridico@hubhealthmed.com.br
Correção de dados incompletos, inexatos ou desatualizados	Até 15 dias corridos	luciana.juridico@hubhealthmed.com.br
Anonimização, bloqueio ou eliminação de dados desnecessários ou tratados em desconformidade	Até 15 dias corridos, ressalvada retenção obrigatória por lei	luciana.juridico@hubhealthmed.com.br
Portabilidade dos dados	Conforme regulamentação específica da ANPD sobre portabilidade, quando aplicável	luciana.juridico@hubhealthmed.com.br
Revogação do consentimento	Imediato, com cessação do respectivo tratamento	luciana.juridico@hubhealthmed.com.br
Informação sobre compartilhamento de dados	Até 15 dias corridos	luciana.juridico@hubhealthmed.com.br

11. Avaliação de Necessidade, Adequação e Proporcionalidade

Critério	Avaliação
Necessidade	Apenas os dados estritamente necessários a cada finalidade específica são coletados; campos não essenciais não são exigidos em formulários e cadastros.
Adequação	Há coerência entre os dados tratados e as finalidades declaradas (execução contratual, faturamento, entrega e comunicação institucional), sem desvio de finalidade constatado.
Minimização	Revisão periódica dos campos de cadastro no ERP TOTVS e no CRM, com descontinuação de campos não utilizados nos últimos 24 meses.
Não reutilização incompatível	Os dados não são utilizados para finalidades diversas das originalmente informadas ao titular, sem base legal ou consentimento específico para tanto.
Qualidade dos dados	Existência de rotina de atualização cadastral vinculada aos processos comercial e de faturamento, reduzindo o risco de dados desatualizados.

12. Análise de Riscos

Referência metodológica: ABNT NBR ISO/IEC 29134:2017, seção 6.4.4, combinada com os critérios de estimativa de risco da ABNT NBR ISO/IEC 27005:2022. A classificação de probabilidade e impacto segue os parâmetros definidos na Seção 3.1.

Classificação	Faixa de valor (P + I)	Valores possíveis nesta faixa
Baixo	10	5 + 5
Moderado	20 a 30	5 + 15 | 15 + 15
Alto	35 a 60	5 + 30 | 15 + 30 | 30 + 30

Risco identificado	Ameaça / vulnerabilidade	Impacto potencial	Probabilidade	Impacto	Nível de risco
Acesso não autorizado a dados de clientes e fornecedores no ERP/CRM	Controle de acesso insuficiente; compartilhamento de credenciais; ausência de revisão periódica de perfis.	Vazamento de dados, fraude, dano reputacional e sancionamento pela ANPD	Moderado (15)	**Alto (30)**	**Alto (45)**
Compartilhamento com terceiros sem cláusula de proteção de dados	Contratação de operadores (transportadoras, fabricantes) sem *due diligence* formal de privacidade	Responsabilização solidária, dano ao titular e descumprimento dos arts. 46 a	Baixo (5)	**Moderado (15)**	**Moderado (20)**

Risco identificado	Ameaça / vulnerabilidade	Impacto potencial	Probabilidade	Impacto	Nível de risco
		48 da LGPD (medidas de segurança, confidencialidade e comunicação de incidentes)			
Armazenamento sem criptografia adequada em repouso e em trânsito	Configuração inadequada de banco de dados; ausência de cifragem em backups	Perda, roubo ou exposição de dados; violação de segurança de larga escala	Moderado (15)	Alto (30)	Alto (45)
Ausência de registro de consentimento para marketing/comunicação institucional	Falha em manter evidência auditável de consentimento (art. 8º, LGPD)	Descumprimento da LGPD; impossibilidade de comprovar licitude do tratamento perante fiscalização	Baixo (5)	Moderado (15)	Moderado (20)
Transferência internacional de dados sem fundamento formalizado	Compartilhamento incidental de contatos com matrizes estrangeiras de fabricantes, sem cláusula-padrão ou avaliação de adequação	Transferência irregular nos termos do Regulamento CD/ANPD nº 19/2024; risco sancionador	Moderado (15)	Alto (30)	Alto (45)
Atraso ou falha na comunicação de incidente de segurança à ANPD	Ausência de plano de resposta a incidentes formalizado e testado, com prazos e responsáveis definidos	Sanção administrativa por descumprimento do dever de comunicação (Resolução CD/ANPD nº 15/2024) e agravamento de dano ao titular	Baixo (5)	Alto (30)	Alto (35)
Retenção de dados além do prazo necessário	Ausência de rotina automatizada de expurgo/anonimização em sistemas legados	Aumento da superfície de exposição em caso de incidente; descumprimento do princípio da necessidade	Baixo (5)	Alto (30)	Alto (35)
Uso de dados de representantes de órgãos públicos além da finalidade licitatória	Reaproveitamento de base de contatos governamentais para finalidades comerciais não relacionadas ao certame de origem	Desvio de finalidade (art. 6º, I, LGPD); dano institucional em relação contratual com o Poder Público	Baixo (5)	Moderado (15)	Moderado (20)

13. Plano de Tratamento e Mitigação de Riscos

O plano a seguir formaliza as ações corretivas e preventivas necessárias para reduzir os riscos identificados na Seção 12 a um nível residual aceitável, com responsáveis e prazos definidos, permitindo o acompanhamento pela Diretoria e pelo Encarregado.

Risco (ref.)	Ação de tratamento	Responsável	Prazo	Risco residual esperado
Acesso não autorizado (ERP/CRM)	Implementar revisão trimestral de perfis de acesso e autenticação multifator obrigatória para todos os módulos que tratem dados pessoais	TI / Compliance	Contínuo, com primeira revisão em até 90 dias	Moderado (15–20)
Compartilhamento sem cláusula de proteção de dados	Padronizar cláusula de proteção de dados pessoais em todos os contratos com operadores (transportadoras, fabricantes, contabilidade) e implementar checklist de *due diligence* de terceiros	Jurídico e Compliance	180 dias	Baixo (5–10)
Armazenamento sem criptografia adequada	Validar e documentar criptografia em repouso e em trânsito para bases que contenham dados pessoais, incluindo backups segregados	TI	120 dias	Moderado (15)
Ausência de registro de consentimento	Implementar mecanismo técnico de registro e versionamento do consentimento (data, hora, texto aceito, canal) no CRM	TI / Comercial	120 dias	Baixo (5–10)
Transferência internacional sem fundamento formalizado	Elaborar inventário de transferências internacionais e adotar cláusulas-padrão contratuais da ANPD ou cláusulas específicas; comunicar imediatamente os fabricantes multinacionais sobre a necessidade de adequação	Jurídico e Compliance	90 dias (antecipado de 180 dias, em razão da reclassificação para alto)	Moderado (20)
Comunicação de incidentes à ANPD	Formalizar e testar Plano de Resposta a Incidentes de Segurança, alinhado à Resolução CD/ANPD nº 15/2024, com matriz de severidade e prazos internos de escalonamento	TI / Jurídico e Compliance	90 dias	Baixo (10)

Risco (ref.)	Ação de tratamento	Responsável	Prazo	Risco residual esperado
Retenção além do necessário	Implementar rotina automatizada de expurgo/anonimização de dados inativos há mais de 5 anos	TI	90 dias (antecipado de 180 dias, em razão da reclassificação para alto)	Baixo (10)
Uso de dados públicos além da finalidade licitatória	Segregar bases de contatos governamentais por finalidade (licitação x prospecção comercial), com trava de reutilização não autorizada	Comercial / TI	120 dias	Baixo (5–10)

14. Medidas de Mitigação e Controles de Segurança

14.1. Medidas técnicas

- Acesso com autenticação multifator e senha, com política de complexidade mínima e expiração periódica;
- Controle de acesso baseado em perfis funcionais (RBAC), com concessão segundo o princípio do menor privilégio;
- Firewall, antivírus corporativo e ferramentas de detecção de intrusão;
- Criptografia de dados pessoais em trânsito e, sempre que tecnicamente viável, em repouso;
- Backup diário com cópias segregadas e testes periódicos de restauração;
- Registro (log) de acessos e alterações em bases que contenham dados pessoais, com retenção adequada para fins de auditoria e investigação de incidentes.

14.2. Medidas administrativas

- Treinamento periódico dos colaboradores sobre proteção de dados pessoais e segurança da informação;
- Política de Segurança da Informação e Política de Privacidade aprovadas pela Diretoria e revisadas anualmente;
- Auditorias internas sobre o programa de privacidade;
- Contratos com cláusulas específicas de proteção de dados pessoais e de responsabilização de operadores;
- Procedimento formal de *due diligence* de privacidade e segurança na contratação de novos operadores/terceiros.

14.3. Medidas organizacionais

- Encarregado (DPO) formalmente designado, com canal de comunicação direto e público;
- Procedimento de resposta a incidentes de segurança, com plano de contenção, erradicação e comunicação, alinhado à Resolução CD/ANPD nº 15/2024;
- Processo de revisão de terceiros (*due diligence*) previamente à contratação e durante a vigência contratual;
- Comitê ou rito interno de privacidade para deliberação sobre novos tratamentos e alterações relevantes de finalidade.

14.4. Privacy by Design e Privacy by Default

Em atendimento ao art. 46, §2º, da LGPD, a Companhia observa o princípio de Privacy by Design e Privacy by Default na concepção de novos produtos, serviços e processos que envolvam dados pessoais. A avaliação de privacidade deve ocorrer, no mínimo, nos seguintes momentos: (i) antes da contratação de novos sistemas ou fornecedores de tecnologia que tratem dados pessoais; (ii) antes da implantação de novos processos de coleta de dados ou da alteração de finalidade de processos já existentes; e (iii) antes de projetos de integração entre sistemas que envolvam compartilhamento de dados pessoais. Nessas hipóteses, a área de TI deverá consultar previamente o Encarregado e a área de Jurídico e Compliance, que avaliarão a necessidade de RIPD específico.

15. Gestão de Incidentes de Segurança

A Companhia adota protocolo de gestão de incidentes de segurança que possam afetar dados pessoais, estruturado em fases de detecção, contenção, avaliação de severidade, comunicação e lições aprendidas. A avaliação de severidade observa os critérios de risco relevante estabelecidos na Resolução CD/ANPD nº 15/2024, que disciplina o Regulamento de Comunicação de Incidentes de Segurança no âmbito da LGPD, definindo prazo e conteúdo mínimo da comunicação à ANPD e aos titulares afetados quando constatado risco ou dano relevante.

Critério de severidade	Gatilho	Ação
Incidente sem risco relevante ao titular	Evento contido, sem exposição efetiva de dados pessoais a terceiros não autorizados	Registro interno, análise de causa-raiz e ação corretiva; comunicação à ANPD dispensada, sem prejuízo do dever de documentação
Incidente com risco relevante ao titular	Exposição, vazamento ou acesso não autorizado a dados pessoais capaz de acarretar dano relevante aos titulares (volume de titulares, natureza do dado, facilidade de identificação, gravidade e ampla divulgação)	Comunicação à ANPD e, quando cabível, aos titulares afetados, no prazo estabelecido pela Resolução CD/ANPD nº 15/2024, com conteúdo mínimo definido no regulamento (descrição da natureza dos dados, titulares afetados, medidas técnicas adotadas e riscos envolvidos)

16. Due Diligence de Terceiros e Operadores

Previamente à contratação de operadores que tratem dados pessoais em nome da Hub Health (transportadoras, escritório de contabilidade, plataformas de pagamento, fornecedores de tecnologia), a área de Jurídico e Compliance realiza avaliação de *due diligence* contemplando: (i) existência de política de privacidade e de segurança da informação do terceiro; (ii) capacidade de atendimento a incidentes de segurança dentro dos prazos regulatórios; (iii) inclusão de cláusulas contratuais específicas de proteção de dados pessoais, sub-rogação de responsabilidade e auditoria; e (iv) verificação de eventual necessidade de cláusulas-padrão de transferência internacional, quando o terceiro estiver localizado ou processar dados fora do território nacional.

17. Análise da Necessidade de Comunicação Prévia à ANPD

Com base na matriz de riscos apresentada na Seção 12 e no plano de tratamento da Seção 13, cinco dos oito riscos remanescentes classificam-se como altos após a correção metodológica desta Versão 2.0, todos com plano de tratamento formalizado, responsáveis e prazos definidos (a maioria em até 90 dias). Essa classificação, por si só, não impõe comunicação prévia e específica à ANPD sobre o tratamento como um todo, nos termos do art. 38, parágrafo único, da LGPD, tratando-se de risco identificado, mensurado e em mitigação ativa — o que é o próprio objetivo do RIPD. Ressalva-se, contudo, que: (i) qualquer incidente de segurança que configure risco ou dano relevante aos titulares deverá ser comunicado à ANPD e aos titulares afetados na forma da Resolução CD/ANPD nº 15/2024, independentemente da conclusão deste RIPD; e (ii) este documento será revisado sempre que houver tratamento de dados sensíveis em larga escala, alteração relevante de finalidade, determinação da ANPD nesse sentido, ou o vencimento dos prazos do plano de tratamento sem a devida implementação.

18. Conclusão e Recomendações

Este RIPD demonstra que o tratamento avaliado permanece alinhado aos princípios da LGPD. A Versão 2.0 incorpora as correções apontadas em análise jurídica de auditoria interna realizada em julho de 2026, com destaque para: (i) a padronização da metodologia de cálculo de risco, com reclassificação de três riscos anteriormente subavaliados; (ii) a formalização do teste de legítimo interesse (LIA) como Anexo II; (iii) a inclusão de campo de controle da comunicação da indicação do DPO à ANPD; (iv) a antecipação dos prazos de mitigação da transferência internacional de dados; (v) a correção de referência legal na matriz de riscos; (vi) a referência ao ROPA como Anexo III; e (vii) a inclusão do mapeamento de rastreabilidade sanitária (ANVISA) e do princípio de Privacy by Design.

Com as correções implementadas, a classificação de risco do tratamento passa a ser predominantemente Alta em 5 dos 8 riscos mapeados (antes 2 de 8), o que reforça - e não fragiliza - a robustez do programa de privacidade da Companhia, por tornar a matriz de riscos mais fiel à real severidade dos cenários identificados e por direcionar prioridade de tratamento às áreas que efetivamente demandam atenção imediata (transferência internacional, comunicação de incidentes e retenção de dados).

19. Revisão e Atualização do Documento

Este RIPD será revisado, no mínimo, anualmente, ou sempre que ocorrer: (i) alteração relevante de finalidade, de categoria de dados tratados ou de titulares envolvidos; (ii) incidente de segurança que evidencie a necessidade de reavaliação de controles; (iii) alteração normativa relevante editada pela ANPD ou por legislação superveniente; ou (iv) determinação da ANPD ou de autoridade competente. A responsabilidade pela condução do processo de revisão é do Encarregado (DPO), em conjunto com a área de Jurídico e Compliance, com validação final da Diretoria da Companhia.

Anexo I. Glossário

Termo	Definição
ANPD	Autoridade Nacional de Proteção de Dados, órgão da administração pública federal responsável por zelar pela proteção de dados pessoais e fiscalizar o cumprimento da LGPD.
Controlador	Pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI, LGPD).
Operador	Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII, LGPD).
Encarregado (DPO)	Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares e a ANPD (art. 5º, VIII, LGPD).
RIPD / DPIA	Documentação que descreve os processos de tratamento de dados pessoais capazes de gerar riscos às liberdades civis e aos direitos fundamentais, contendo, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco (art. 5º, XVII, LGPD).
Titular	Pessoa natural a quem se referem os dados pessoais objeto de tratamento (art. 5º, V, LGPD).
Risco residual	Nível de risco remanescente após a aplicação de controles e medidas de mitigação.
Legítimo interesse	Base legal prevista no art. 7º, IX, da LGPD, disciplinada pelo art. 10, que autoriza o tratamento para finalidades legítimas do controlador, mediante teste de proporcionalidade e respeito aos direitos e expectativas do titular.
LIA (Legitimate Interest Assessment)	Teste de proporcionalidade exigido pelo art. 10, §2º, da LGPD para fundamentar o tratamento baseado em legítimo interesse, avaliando a finalidade legítima, a necessidade do tratamento e o balanceamento entre os interesses do controlador e os direitos e liberdades fundamentais do titular.
ROPA / RAT	Registro das Operações de Tratamento de Dados Pessoais (Record of Processing Activities), inventário de todas as atividades de tratamento realizadas pela organização, exigido pelo art. 37 da LGPD.

Anexo II. Teste de Legítimo Interesse (LIA) — Síntese

Em atendimento ao art. 10, §2º, da LGPD e à recomendação de auditoria interna registrada no controle de versões (Seção 0), apresenta-se a síntese do teste de proporcionalidade (Legitimate Interest Assessment) aplicado ao tratamento fundamentado no art. 7º, IX c/c art. 10, da LGPD. O documento completo do LIA, com a memória de avaliação detalhada, é mantido como registro autônomo pela área de Jurídico e Compliance e disponibilizado ao Encarregado e à ANPD, caso solicitado.

Elemento do teste	Análise
Finalidade legítima invocada	Prospecção comercial (leads), atendimento e relacionamento pós-venda, prevenção a fraudes e análise de satisfação de clientes.
Necessidade	O tratamento é necessário para viabilizar o relacionamento comercial contínuo com clientes e potenciais clientes, não havendo meio alternativo menos invasivo igualmente eficaz para as finalidades indicadas.
Expectativa legítima do titular	Clientes e potenciais clientes que interagem comercialmente com a Companhia podem razoavelmente esperar o tratamento de seus dados de contato para fins de relacionamento comercial e pós-venda.
Balanceamento (teste de proporcionalidade)	Os benefícios do tratamento para a Companhia (eficiência comercial, prevenção a fraudes) não se sobrepõem de forma desproporcional aos direitos e liberdades fundamentais dos titulares, que permanecem resguardados pelo direito de oposição e pelos demais direitos do art. 18 da LGPD.
Salvaguardas adotadas	Canal de atendimento e de oposição ao tratamento disponibilizado ao titular; controles de acesso e segurança descritos na Seção 14; revisão periódica da base de dados para eliminação de contatos inativos.
Conclusão do teste	O tratamento com base em legítimo interesse é considerado adequado e proporcional para as finalidades indicadas, devendo ser reavaliado a cada revisão anual deste RIPD ou sempre que houver alteração relevante de finalidade.

Anexo III. Registro das Operações de Tratamento (ROPA) — Referência

O inventário completo de todas as atividades de tratamento de dados pessoais da Partner Farma, da Átons do Brasil e da Hub Health - incluindo, além da atividade avaliada neste RIPD, as atividades de Recursos Humanos, Compras/Fornecedores, Marketing, Tecnologia da Informação, Financeiro, Facilities e Compliance - está consolidado no documento "Registro das Operações de Tratamento de Dados Pessoais (ROPA)", mantido em planilha própria pela área de Jurídico e Compliance, atualizada em conjunto com o Encarregado e revisada com a mesma periodicidade deste RIPD (Seção 19).

O ROPA deve ser consultado sempre que se fizer necessária a visão consolidada das atividades de tratamento da Companhia para fins de accountability (art. 6º, X, e art. 37, da LGPD), auditoria interna ou resposta a eventual fiscalização da ANPD.

(Página de assinatura do Relatório de Impacto à Proteção de Dados da empresa Hub Health Distribuidora de Produtos Hospitalares Ltda. - Versão 2.0/2026).

Fortaleza, Ceará – 01 de agosto de 2026.

mario@hubhealthmed.com.br
D4Sign
Assinado

Mario Kanashiro Filho

Responsável Legal

luciana.juridico@hubhealthmed.cc
D4Sign
Luciana Alves Campos
Assinado

Luciana Alves Campos

Responsável / Encarregada (DPO)

agatha.juridico@hubhealthmed.cc
D4Sign
Assinado

Agatha Rosa Gomes

Testamunha

georgia.rh@qeri.srv.br
D4Sign
Georgia Palagi Kanashiro
Assinado

Georgia Palagi Kanashiro

Testemunha

01 RELATORIO DE IMPACTO A PROTECAO DE DADOS HUB HEALTH pdf

Código do documento 155f3abb-fef9-4eb2-97cb-1939158d9562

Assinaturas

Luciana Alves Campos
luciana.juridico@hubhealthmed.com.br
Assinou como parte

Agatha Rosa Gomes
agatha.juridico@hubhealthmed.com.br
Assinou como testemunha

Georgia Palagi Kanashiro
georgia.rh@geri.srv.br
Assinou como testemunha

Mario Kanashiro Filho
mario@hubhealthmed.com.br
Assinou como parte

Eventos do documento

21 Jul 2026, 10:33:48
Documento 155f3abb-fef9-4eb2-97cb-1939158d9562 **criado** por MARIO KANASHIRO FILHO (bbd1ea4b-9999-4902-9b23-409d7d5b9c92). Email:luciana.juridico@partnerfarma.com.br. - DATE_ATOM: 2026-07-21T10:33:48-03:00

21 Jul 2026, 10:34:16
MARIO KANASHIRO FILHO (bbd1ea4b-9999-4902-9b23-409d7d5b9c92). Email: luciana.juridico@partnerfarma.com.br. **REMOVEU** o signatário **luciana.juridico@partnerfarma.com.br** - DATE_ATOM: 2026-07-21T10:34:16-03:00

21 Jul 2026, 10:40:11
Assinaturas **iniciadas** por MARIO KANASHIRO FILHO (bbd1ea4b-9999-4902-9b23-409d7d5b9c92). Email: luciana.juridico@partnerfarma.com.br. - DATE_ATOM: 2026-07-21T10:40:11-03:00

21 Jul 2026, 10:41:30
AGATHA ROSA GOMES **Assinou como testemunha** - Email: agatha.juridico@hubhealthmed.com.br - IP: 200.206.172.99 (200-206-172-99.dsl.telesp.net.br porta: 6186) - Geolocalização: -23.533885455017817 -47.48625053029081 - Documento de identificação informado: 493.062.348-05 - DATE_ATOM: 2026-07-21T10:41:30-03:00

21 Jul 2026, 15:58:21
LUCIANA ALVES CAMPOS **Assinou como parte** - Email: luciana.juridico@hubhealthmed.com.br - IP: 200.206.172.99 (200-206-172-99.dsl.telesp.net.br porta: 29430) - Geolocalização: -23.49994041888804 -46.60990695424831 - Documento de identificação informado: 166.721.968-54 - DATE_ATOM: 2026-07-21T15:58:21-03:00

22 Jul 2026, 17:38:10
MARIO KANASHIRO FILHO **Assinou como parte** - Email: mario@hubhealthmed.com.br - IP: 93.62.77.166 (93-62-77-166.ip21.fastwebnet.it porta: 59778) - Geolocalização: 43.77427851507912 11.251443279648129 - Documento de identificação informado: 164.285.718-11 - DATE_ATOM: 2026-07-22T22:38:10+02:00

31 Jul 2026, 11:47:12
GEORGIA PALAGI KANASHIRO **Assinou como testemunha** - Email: georgia.rh@geri.srv.br - IP: 200.206.172.99 (200-206-172-99.dsl.telesp.net.br porta: 64110) - Documento de identificação informado: 149.716.428-11 - DATE_ATOM: 2026-07-31T11:47:12-03:00

Hash do documento original
(SHA256):ef0d7bb9c6cff6f02b3bf4b4510e62a353c0d944c0b021f641e9e938f40b0971
(SHA512):88d60f003e44199230cde503340a4f9a5a4e811d9bb975cba28fb12bd75db79fca3d2a148a6db3897ae1b0f4ac19a5e7f2a107cedd284d8ddc43c3c6df99164e

Esse log pertence **única** e **exclusivamente** aos documentos de HASH acima

Esse documento está assinado e certificado pela D4Sign
Integridade certificada no padrão ICP-BRASIL
Assinaturas eletrônicas e físicas têm igual validade legal, conforme **MP 2.200-2/2001** e **Lei 14.063/2020**.