RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

FIAP Postech Software Architecture - SOAT 4 - Grupo 23

Histórico de Revisões

Data	Versão	Descrição	Autor
22/07/2024	1.0	Conclusão da primeira versão do relatório	Elen de Souza

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS – RIPD

OBJETIVO

O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os 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 risco.

Referência: Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador Departamento de Segurança	
Operador SOAT 4 GRUPO 23	
Encarregado Elen de Souza	
E-mail Encarregado privacidade@healthmed.com.br	**Telefone Encarregado** +9999 (0) 999 799 9 799

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

O RIPD do Health&Med foi elaborado para os seguintes objetivos:

2.1 Para atendimento à Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) e regulamentações emanadas pela Autoridade Nacional de Proteção de Dados -ANPD.

2.2 Para orientação e direcionamento dos funcionários do Health&Med com relação ao tratamento das informações pessoais de clientes, colaboradores e demais interlocutores, que por necessidade de negócios são coletadas em seus processos formais.

2.3 Para definição de políticas internas de garantia da segurança e governança dos dados pessoais coletados;

2.4 Para garantia de proteção e mitigação de riscos eventualmente envolvidos evitando:

i) ameaças ou riscos à privacidade; à segurança; à integridade e/ou à confidencialidade;

ii) destruição acidental ou ilícita; perda; alteração; divulgação ou acesso não autorizado;

iii) quaisquer outras formas ilegais de tratamento; e

iv) incidentes de segurança ou privacidade.

3 – DESCRIÇÃO DO TRATAMENTO

Os sistemas e processos do Health&Med foram desenhados para a captação somente dos dados que se fazem pertinentes para a elaboração de contratos comerciais; cadastro de clientes e fornecedores; informações para atendimentos a demandas fiscais e legais; registros de funcionários e para ações de marketing

3.1 – NATUREZA DO TRATAMENTO

3.1.1 Os dados pessoais são coletados mediante preenchimento de formulário eletrônico do Health&Med pelo titular dos dados pessoais. Os dados são transferidos e armazenados nos servidores cloud na Amazon Web Services (AWS), administrados pelo Health&Med e localizados no Norte da Virginia, nos EUA.

3.1.2 A fonte de dados é o titular dos dados pessoais mediante o preenchimento de formulário eletrônico do Health&Med.

3.1.3 O operador de dados pessoais é a administração da empresa Health&Med (SOAP4 GRUPO 23), o qual é responsável pela implementação do sistema que automatiza todas as

operações de tratamento de dados pessoais (Coleta, Retenção, Processamento, Compartilhamento e Eliminação).

3.1.4 As medidas de segurança atualmente adotadas são: Controle de Acesso Lógico, Controles Criptográficos, Controles de Segurança em Redes, Proteção Física e do Ambiente.

3.2 – ESCOPO DO TRATAMENTO

3.2.1 Os dados pessoais tratados pelo Health&Med abrangem: - Informações de identificação pessoal: Nome, e-mail, CPF, CRM. Além de informações de saúde, como resultados de exames, diagnósticos, histórico de doenças, laudos médicos.

3.2.2 Os dados coletados de acordo com o item 3.2.1 são para estrito cumprimento de relações comerciais, contratuais e legais, protegidos por cláusulas de sigilo. Todo funcionário do Health&Med é treinado e assina termo de ciência com relação às informações;

3.2.3 A frequência de tratamento dos dados pessoais e das informações de saúde é 24x7 (24 horas por dia nos 7 dias da semana).

3.2.4 Os dados pessoais obtidos serão mantidos armazenados durante a existência da empresa. Esse período de armazenamento poderá ser revisto em alinhamento a qualquer nova disposição legal sobre prazo de retenção.

3.2.5 A abrangência do tratamento de dados pessoais é nacional para manutenção do cadastro único dos clientes.

3.3 – CONTEXTO DO TRATAMENTO

3.3.1 Qualquer coleta de dados pessoais é avisada ao titular através de documentos informativos no site do Health&Med no contato via e-mail organizacional e por aditivos de contrato, no caso de funcionários;

3.3.2 A política de sigilo da organização garante ciência por parte de todos os colaboradores do cuidado no trato com as informações pessoais e na proibição de qualquer compartilhamento sem o consentimento pessoal do titular e da organização.

3.3.3 O Health&Med utiliza recursos de segurança robustos para evitar qualquer acesso indevido em sua base de dados.

3.3.4 Qualquer atualização, compartilhamento dos dados pessoais ou acessos suspeitos são avisados ao titular. Embora os campos Nome, CPF, e-mail e CRM sejam restritos para alteração, o titular pode requisitar informações sobre seus dados pessoais a qualquer momento.

3.4 – FINALIDADE DO TRATAMENTO

A finalidade para a coleta de dados pessoais pelo Health&Med atende exclusivamente:

3.4.1 O cumprimento de obrigação legal fiscal, comercial ou regulatória;

3.4.2 Execução de contrato de consultas médicas e outros contratos, assim como de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

3.4.3 Atender aos interesses legítimos para o pleno funcionamento da organização.

Para a elaboração do presente documento foram consultados representantes internos da organização; consultores jurídicos e analistas das empresas que prestam serviços de armazenamento de informações através das ferramentas contratadas, bem como necessidade de consumidores, clientes e prestadores.

4 – PARTES INTERESSADAS CONSULTADAS

4.1 Especialistas em Segurança da Informação da Health&Med: Consultados para identificar possíveis melhorias na proteção dos dados pessoais tratados.

4.2 Consultor Jurídico: Responsável por avaliar a conformidade do tratamento de dados com os requisitos legais da LGPD.

4.3 Gestores e Funcionários da Health&Med: Consultados para obter informações técnicas e administrativas sobre os processos de trabalho realizados.

4.4 Responsável pelo Tratamento de Dados Pessoais: Coordenou o levantamento e avaliou as informações técnicas, administrativas, legais e de riscos fornecidas pelas demais partes consultadas.

4.5 Serviços de Terceiros (Google Agenda e Google Meetings): Considerados na análise de riscos

relacionados ao uso de plataformas externas para agendamento e realização de consultas online.

4.6 Equipe de Desenvolvimento de Software da Health&Med: Consultada para fornecer detalhes sobre a arquitetura técnica e medidas de segurança implementadas no novo sistema de Telemedicina.

5 – NECESSIDADE E PROPORCIONALIDADE

5.1 – FUNDAMENTAÇÃO LEGAL

5.1.1 A base legal para o tratamento de dados pessoais é o artigo 7º, inciso I da LGPD: "com o consentimento explícito do titular"; e inciso II da LGPD: "para o cumprimento de uma obrigação legal ou regulatória pelo controlador".

5.2 – QUALIDADE E MINIMIZAÇÃO DOS DADOS

5.2.1 A escolha dos dados a serem coletados para a implementação dos processos da Health&Med foi baseada na premissa de coletar o mínimo necessário de dados pessoais para a execução de suas atividades, incluindo a realização de consultas online e o agendamento de compromissos.

5.3 – MEDIDAS PARA ASSEGURAR CONFORMIDADE DO OPERADOR

5.3.1 Em intervalos programados, a Health&Med realiza auditorias internas sobre as práticas de segurança de suas plataformas, conduzidas por especialistas qualificados, para garantir a conformidade com as diretrizes estabelecidas.

5.3.2 Internamente, o acesso aos sistemas que administram e armazenam os dados pessoais é protegido por uma política de senhas exclusivas e individuais.

5.3.3 Tanto o sistema de segurança quanto a política de confidencialidade asseguram o tratamento apropriado das informações coletadas, permitindo ações corretivas em caso de qualquer incidente.

5.4 – MEDIDAS PARA ASSEGURAR DIREITOS DO TITULAR DOS DADOS

5.4.1 Os sistemas da Health&Med estão configurados para que os titulares dos dados possam exercer os direitos previstos no artigo 18º da LGPD. A Política de Privacidade detalha esses direitos e pode ser consultada em healthmed.com.br/politica-privacidade.

5.4.2 Caso um usuário identifique qualquer falha ou vulnerabilidade de segurança no sistema, ele pode reportá-la através do e-mail privacidade@healthmed.com.br.

5.4.3 Quando solicitado pelo titular dos dados, a Health&Med fornecerá informações sobre a privacidade (confirmação de existência ou acesso aos dados pessoais) por e-mail ou em formato impresso, conforme a solicitação.

5.5 – SALVAGUARDAS PARA AS TRANSFERÊNCIAS INTERNACIONAIS DE DADOS

5.5.1 O armazenamento de dados em servidores internacionais e a subsequente transferência para fora do país estão de acordo com o artigo 33º da LGPD, que define as permissões para transferências internacionais de dados pessoais.

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

6.1 Para identificar e avaliar os riscos associados ao tratamento de dados pessoais na Health&Med, foi empregada a Matriz Impacto x Probabilidade. Esta abordagem permite determinar o nível de risco e definir as medidas e salvaguardas necessárias para mitigação.

6.2 Para cada risco identificado, são avaliados a probabilidade de ocorrência e o impacto caso o evento se concretize, analisando o potencial de risco.

6.3 Os níveis de probabilidade e impacto são multiplicados para calcular os níveis de risco, que orientarão a implementação das medidas de segurança apropriadas, conforme os critérios estabelecidos.

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Exposição não autorizada de dados sensíveis	5	15	75
R02	Falha na anonimização de informações pessoais	5	10	50
R03	Deficiência na atualização dos consentimentos	10	15	150
R04	Vazamento de dados de clientes	5	15	75
R05	Uso indevido de dados para marketing direto	10	15	150
R06	Inadequação na gestão de cookies e rastreamento	5	10	50
R07	Acesso indevido por funcionários internos	10	15	150
R08	Retenção excessiva de dados de clientes	15	15	225
R09	Falha na implementação de medidas de segurança física	5	15	75
R10	Incidente de segurança em fornecedor de serviços	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade.	5	10	50
R12	Roubo.	10	15	150
R13	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
R14	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75

* verde, é entendido como baixo;
* amarelo, representa risco moderado; e
* vermelho, indica risco alto.

7 – MEDIDAS PARA TRATAR OS RISCOS

Risco	Medida(s)	Efeito sobre o Risco[1]	Risco Residual[2]			Medida(s)[3] Aprovada(s)
			P	I	Nível (P x I)	
R01 - Acesso não autorizado	Implantação de uma política de acesso às informações.	Evitar	5	15	75	Sim

R03 - Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento	Incluir cláusulas específicas sobre o tratamento e	Evitar	5	5	25	Sim

do titular dos dados pessoais.	compartilhamento de dados pessoais.					
R04 - Falha na proteção dos direitos de acesso dos titulares de dados	Realizar revisões regulares para garantir o cumprimento dos direitos de acesso dos titulares	Evitar	5	5	25	Sim
R05 - Erro durante o processamento de dados pessoais	Implementar procedimentos de validação para assegurar a integridade do processamento de dados	Reduzir	5	15	75	Sim
R07 - Modificação não autorizada de dados pessoais	Implementar controles robustos de autenticação e autorização para prevenir modificações não autorizadas	Evitar	5	15	75	Sim
R08 - Perda de dados pessoais por falta de backups adequados	Manter backups frequentes e um plano de recuperação de desastres para mitigar perdas de dados	Reduzir	5	15	75	Sim
R09 - Reidentificação indevida de dados pseudonimizados	Implementar técnicas avançadas de pseudonimização e restrições rigorosas de acesso aos dados pseudonimizados	Evitar	5	5	25	Sim
R10 - Exclusão não autorizada de dados pessoais	Manter registros detalhados de operações de exclusão e monitorar atividades suspeitas para detectar exclusões	Evitar	5	10	50	Sim

	não autorizadas					
R12 - Roubo de dados pessoais por acesso não autorizado	Implementar restrições estritas de acesso e criptografia de dados para prevenir roubos de dados .	Evitar	5	15	75	Sim
R13 - Tratamento de dados sem o consentimento explícito do titular	Obter consentimento explícito dos titulares antes de qualquer tratamento de dados e manter políticas de privacidade atualizadas	Evitar	5	5	25	Sim

	privacidade acessível e compreensível					
R14 - Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	Adotar medidas que preservem a privacidade e a confidencialidade desses dados com a pseudonimização correta dos dados pessoais.	Evitar	5	5	25	Sim

Legenda:

[1] Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: **Reduzir**, **Evitar**, **Compartilhar** e **Aceitar**.

[2] Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratar o risco.

[3] Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

8 – APROVAÇÃO

Rúbrica

Responsável pela elaboração do RIPD

Rúbrica

Encarregado

Rúbrica

Autoridade
Representante do Controlador

Rúbrica

Autoridade
Representante do Operador