NORMA DE AVALIAÇÃO DE IMPACTO

1. INTRODUÇÃO

1.1. O **HOSPITAL NOSSA SENHORA DA CONCEIÇÃO S.A.** (matriz), aqui representando as demais filiais que compõem o chamado Grupo Hospitalar Conceição ("**GHC**"), em atendimento à LGPD, elaborou a presente norma de avaliação de impacto para elaboração de Relatório de Impacto à Proteção de Dados (RIPD) quando da realização de operações que impactem significativamente os dados tratados pelo **GHC**.

1.2. A LGPD conceitua, em seu art. 5, inciso XVII, o RIPD como sendo a **"documentação do controlador 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 risco"**.

1.3. O RIPD visa o registro, regularidade e a legalidade nas operações de tratamento de dados pessoais, comprovando o estudo e planejamento desenvolvido pelo **GHC**, com o objetivo de realizar uma operação de tratamento de dados pessoais de forma prudente e visando eliminar ou minimizar os potenciais efeitos adversos trazidos pela operação referida.

1.4. Ainda, a LGPD aponta quais informações deve conter um RIPD (o art. 38, parágrafo único):

a) A análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados;
b) A metodologia utilizada para a coleta e para a garantia da segurança das informações;
c) Descrição dos tipos de dados coletados.

1.5. Ademais, a Autoridade Nacional de Proteção de Dados ("ANPD") poderá, também, solicitar ao controlador a elaboração do Relatório de Impacto à Proteção de Dados Pessoais quando o tratamento for pautado no legítimo interesse do controlador ou em quaisquer outros casos que entender necessários, conforme dispõe o artigo 10, § 3º, e do artigo. 38 da LGPD.

1.6. Todos aqueles que atuam diariamente nas operações do **GHC** devem observar as regras previstas nesta norma e contribuir para a conscientização e disseminação da importância na elaboração do RIPD, incentivando a adoção de uma cultura de proteção de dados pessoais.

1.7. Esta norma e suas atualizações estarão disponíveis junto ao Comitê de Proteção de Dados Pessoais (Comitê) ou no Repositório de Documentos do GHC.

2. PRINCIPAIS ELEMENTOS DE UM PROCESSO/ELABORAÇÃO DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

2.1. O RIPD deve, preferencialmente, ser elaborado durante a etapa inicial do desenvolvimento de um projeto, ou seja, antes de o **GHC** dar início ao tratamento de dados. No entanto, também é recomendável a elaboração do RIPD para as operações de tratamentos de dados pessoais já existentes e que possam envolver riscos às liberdades civis e aos direitos fundamentais.

2.2. O documento deve conter as seguintes etapas:

- **Identificar a necessidade de um RIPD;**
- **Descrever o tratamento;**
- **Avaliar a necessidade e a proporcionalidade;**
- **Identificar e avaliar os riscos;**
- **Identificar medidas para mitigar os riscos.**

2.2.1. É necessária a criação de processo que se adeque ao formato existente na **GHC** para gerenciamento riscos, projetos e operações relacionadas.

3. IDENTIFICAR A NECESSIDADE DE UM RIPD

3.1. Caso o **GHC** possua um projeto, operação ou serviço que envolva o tratamento de dados pessoais que poderá resultar riscos às liberdades civis e aos direitos fundamentais ou impactar, significativamente, a forma de tratamento dos dados pessoais, é necessária a elaboração do RIPD. Caberá ao líder do departamento ou projeto a comunicação com o Comitê através do e-mail dpo@ghc.com.br.

3.2. Nos casos de tratamento de dados pessoais que venham a gerar dúvidas sobre a necessidade ou não na elaboração do RIPD para o tratamento em questão, **recomenda-se** a utilização da listagem de exemplos para ajudá-los na tomada de decisão sobre a elaboração do RIPD, conforme segue:

- Considera-se necessária a análise de questões relacionadas à proteção de dados pessoais desde a fase inicial de desenvolvimento de qualquer projeto significativo que venha a envolver o tratamento de dados pessoais;
- Considera-se a elaboração de RIPD nos casos em que as operações envolvam:
    - Contratação de parte relacionada que venha a ter envolvimento com dados pessoais em grande escala;
    - Realização de perfis em grande escala;
    - Soluções tecnológicas ou organizacionais inovadoras, como, por exemplo, aplicativos;
    - Tratamento com base no interesse legítimo do controlador;
    - Tratamento de alto volume de dados;
    - Tratamento, principalmente o compartilhamento, de dados biométricos ou genéticos em grande escala;
    - Tratamento de dados envolvendo inteligência artificial;
    - Tratamento de dados pessoais que podem resultar em risco de danos físicos no caso de violação de segurança;
    - Tratamento de dados pessoais sem o fornecimento de aviso de privacidade direcionado ao indivíduo em combinação com qualquer um dos critérios das diretrizes nacionais;
    - Tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento;
    - Tratamento de dados relativos a titulares de dados vulneráveis/crianças e adolescentes;
    - Tratamento de dados sensíveis ou dados de natureza altamente pessoal;
    - Tratamento que envolva impedir que os titulares dos dados exerçam um direito ou usem um serviço ou contrato;
    - Uso de tecnologia inovadora em combinação com qualquer um dos critérios de qualquer diretriz sobre o tema.

- Elabora-se um novo RIPD se houver uma alteração na natureza, âmbito, contexto ou objetivos do tratamento;
- Caso seja optado por não se realizar o RIPD, as razões para tal decisão deverão ser documentadas.

4. DESCREVER O TRATAMENTO

Em caso de necessidade de elaboração do RIPD pelo **GHC**, será necessário descrever o modo e a finalidade no uso de dados pessoais. A descrição deverá incluir a natureza, escopo, contexto e objetivos do tratamento, como discriminado abaixo:

a) **Natureza** é o propósito do tratamento dos dados pessoais, devendo ser incluso qual o ciclo de vida dos dados, qual sua origem, como são armazenados, tratados, usados e eliminados;
b) **Escopo** do tratamento é o que o tratamento abrange, ou seja, qual a natureza dos dados pessoais (cadastrais, clínicos, financeiros etc.), o volume e a variedade dos dados pessoais, a sensibilidade dos dados pessoais etc.;
c) **Contexto** do tratamento é o aspecto mais amplo, que inclui fatores internos e externos que podem afetar as expectativas ou o impacto;
d) **Objetivo** do tratamento é a razão pela qual a organização deseja tratar os dados pessoais.

5. AVALIAR A NECESSIDADE E A PROPORCIONALIDADE

Para avaliação da necessidade e da proporcionalidade do tratamento, a organização deverá considerar se seus planos ajudam no alcance do seu propósito e se existe alguma outra maneira razoável de obter os mesmos resultados.

6. IDENTIFICAR E AVALIAR OS RISCOS

6.1. Para identificação e avaliação dos riscos deverá ser considerado o impacto potencial sobre os titulares e qualquer dano que o tratamento desses dados possa causar - seja físico, emocional ou material.

6.2. Para avaliar se o risco é alto, a organização deverá considerar a probabilidade e a gravidade do possível dano. O dano não precisa ser inevitável para ser qualificado como um risco ou alto risco. Deverá ser mais do que remoto, mas qualquer possibilidade significativa de dano muito sério ainda pode ser suficiente para ser qualificada como um risco alto. Da mesma forma, uma alta probabilidade de dano generalizado, mas de menor importância, pode ainda contar como alto risco.

6.3. O **GHC** deve fazer uma avaliação objetiva dos riscos. É útil usar uma matriz estruturada para pensar sobre a probabilidade e gravidade dos riscos:

IMPACTO						
	Muito Alto	10 RM	20 RM	50 RA	80 RE	100 RE
	Alto	8 RB	16 RM	40 RA	64 RA	80 RE
	Médio	5 RB	10 RM	25 RM	40 RA	50 RA
	Baixo	2 RB	4 RB	10 RM	16 RM	20 RM
	Muito Baixo	1 RB	2 RB	5 RB	8 RB	10 RM
		Muito Baixa	Baixa	Média	Alta	Muito Alta
		1	2	5	8	10
		PROBABILIDADE				

Criticidade	Descrição	Peso
Muito baixa	**Improvável.** Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade	**1**
Baixa	**Rara.** De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	**2**
Média	**Possível.** De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	**5**
Alta	**Provável.** De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	**8**
Muito Alta	**Praticamente certa.** De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	**10**

RB (Risco Baixo)	RM (Risco Médio)	RA (Risco Alto)	RE (Risco Extremo)
0 – 9,99	10 – 39,99	40 – 79,99	80 - 100

6.4. A matriz acima mostra uma forma estruturada de avaliação de riscos. O **GHC** poderá utilizar método diferente considerando seus próprios riscos corporativos, como o impacto da ação regulatória, danos à reputação ou perda da confiança pública.

7. IDENTIFICAR MEDIDAS PARA MITIGAR OS RISCOS

Ao identificar os riscos, a organização deverá adotar medidas técnicas e administrativas para mitigar a sua ocorrência.

8. ASSINAR E REGISTRAR OS RESULTADOS

8.1. Ao final do RIPD, deverá estar registrado: **(i)** quais medidas adicionais a organização planeja tomar; **(ii)** se o risco foi eliminado, reduzido ou aceito; **(iii)** o nível geral de "risco residual" após a adoção de medidas adicionais.

8.2. A organização não precisará eliminar todos os riscos, mas deverá decidir quais riscos são aceitáveis em decorrência dos benefícios do tratamento e as dificuldades de mitigação.

8.3. Como parte do processo de aprovação do RIPD, a organização deve buscar e documentar a orientação do Encarregado de Proteção de Dados sobre se o tratamento está em conformidade com a legislação aplicável.

9. APÓS A FINALIZAÇÃO DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS

9.1. Após a finalização do processo de elaboração do RIPD, o documento deverá ser integrado aos planos de projeto do **GHC**. A organização deve identificar quaisquer pontos de ação e quem será responsável por implementá-los. **É necessário que após a implementação a organização monitore o desempenho contínuo do RIPD.**

9.2. Para ajudar na transparência e responsabilidade, e de acordo com o grau de sigilo do Relatório, recomenda-se a publicação do RIPD. A publicação do documento poderá ajudar a fomentar a confiança nas atividades de tratamento do **GHC** e melhorar a capacidade dos indivíduos de exercer seus direitos.

10. PROCEDIMENTO INTERNO PARA ELABORAÇÃO DO RELATÓRIO DE IMPACTO

10.1. As gerências do **GHC** que estiverem desenvolvendo novos procedimentos, serviços ou contratando partes relacionadas que venham a desenvolver algum tratamento de dados pessoais em nome do **GHC** (operadores), deverão informar ao Comitê, para que os integrantes do Comitê, juntamente com o Encarregado de Dados, avaliem a necessidade, ou não, da elaboração do RIPD para o caso concreto. É possível, ainda, que os integrantes do Comitê realizem uma busca ativa de novos procedimentos que estejam sendo desenvolvidos, ou atuem de ofício, caso venham a ter conhecimento de novos casos que possam ensejar o desenvolvimento do RIPD.

10.2. Após a ciência, pelo Comitê, de alguma das hipóteses elencadas acima, este poderá solicitar maiores informações à área responsável pelo processo. Coletados os dados pertinentes, será elaborado o Relatório de Impacto pelo Comitê, em conjunto com o

Encarregado de Dados, sendo que todo o processo de solicitação, resposta dos questionamentos e elaboração do RIPD não deve ultrapassar o prazo de 30 (trinta) dias.

11. ATUALIZAÇÃO E REVISÃO

11.1. A presente norma será revisada sempre que o Comitê entender necessário, podendo ser consultada, a qualquer momento, no site institucional no endereço [www.ghc.com.br/privacidade].