POLÍTICA DE PRIVACIDADE DE DADOS PESSOAIS

1 – Objetivo

A presente política tem por objetivo demonstrar o compromisso do Hospital São Mateus com a privacidade e proteção de dados pessoais que coleta de seus clientes/pacientes, esclarecendo as regras sobre coleta, registro, armazenamento, uso, compartilhamento e eliminação dos dados coletados, dentro do contexto da prestação de serviços da instituição, de acordo com a lei em vigor de nº 13709/2018 ("Lei Geral de Proteção de Dados").

Esta Política de Privacidade foi elaborada em conformidade com a Lei Federal n. 12.965 de 23 de abril de 2014 (Marco Civil da Internet) e com a Lei Federal n. 13.709, de 14 de agosto de 2018 (Lei de Proteção de Dados Pessoais) - LGPD

1.1 - Direitos do cliente/paciente

O Hospital São Mateus se compromete a cumprir as normas previstas na LGPD e GDPR, em respeito aos seguintes princípios:

- Os dados pessoais do cliente/paciente serão processados de forma lícita, leal e transparente (licitude, lealdade e transparência);

- Os dados pessoais do cliente/paciente serão coletados apenas para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades (limitação das finalidades);

- Os dados pessoais do cliente/paciente serão coletados de forma adequada, pertinente e limitada às necessidades do objetivo para os quais eles são processados (minimização dos dados);

- Os dados pessoais do cliente/paciente serão exatos e atualizados sempre que necessário, de maneira que os dados inexatos sejam apagados ou retificados quando possível (exatidão);

- Os dados pessoais do cliente/paciente serão conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados (limitação da conservação);

- Os dados pessoais do cliente/paciente serão tratados de forma segura, protegidos do tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas (integridade e confidencialidade).

O cliente/paciente do Hospital São Mateus possui os seguintes direitos, conferidos pela Lei de Proteção de Dados Pessoais:

- Direito de confirmação e acesso: é o direito do cliente/paciente de obter do Hospital São Mateus a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de acessar os seus dados pessoais;

- Direito de retificação: é o direito do cliente/paciente de obter do Hospital São Mateus, sem demora injustificada, a retificação dos dados pessoais inexatos que lhe digam respeito;

- Direito à eliminação dos dados (direito ao esquecimento): é o direito do cliente/paciente de ter seus dados apagados;

- Direito à limitação do tratamento dos dados: é o direito do cliente/paciente de limitar o tratamento de seus dados pessoais, podendo obtê-la quando contesta a exatidão dos dados, quando o tratamento for ilícito, quando o Hospital São Mateus não precisar mais dos dados para as finalidades propostas e quando tiver se oposto ao tratamento dos dados e em caso de tratamento de dados desnecessários;

- Direito de oposição: é o direito do cliente/paciente de, a qualquer momento, se opor por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, podendo se opor ainda ao uso de seus dados pessoais para definição de perfil de marketing (profiling);

- Direito de portabilidade dos dados: é o direito do cliente/paciente de receber os dados pessoais que lhe digam respeito e que tenha fornecido ao Hospital São Mateus, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outra instituição;

- Direito de não ser submetido a decisões automatizadas: é o direito do cliente/paciente de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis (profiling), que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

O cliente/paciente poderá exercer os seus direitos por meio de comunicação escrita enviada ao Hospital São Mateus com o assunto *"LGPD-Hospital São Mateus"*, especificando:

- Nome completo ou razão social, número do CPF (Cadastro de Pessoas Físicas, da Receita Federal do Brasil) ou CNPJ (Cadastro Nacional de Pessoa Jurídica, da Receita Federal do Brasil) e endereço de e-mail do cliente/paciente e, se for o caso, do seu representante;

- Direito que deseja exercer junto ao Hospital São Mateus;

- Data do pedido e assinatura do cliente/paciente;

- Todo documento que possa demonstrar ou justificar o exercício de seu direito.

O pedido deverá ser enviado ao e-mail: dpo@hsaomateus.org, ou por correio, ao seguinte endereço e aos cuidados de Daniel Badinhani – Encarregado pelo tratamento de dados pessoais:

Hospital São Mateus
SRES Quadra 2 Lote 1 - Área Especial A1
Cruzeiro Velho
Brasília - DF
CEP: 70.648-010

2 – Definições

2.1 – Dados Pessoais

Dados relacionados a uma pessoa física identificada ou identificável.

2.2 – Dados Sensíveis

Dados pessoais que façam referência a convicção religiosa, condição de saúde, origem racial ou étnica, vida e orientação sexual, filiação a sindicato ou organização política, crenças de ordem religiosa ou filosófica, dado genético ou biométrico quando vinculado a uma pessoa física.

2.3 – Anonimização

Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meios dos quais um dados pessoal perde a possibilidade de associação, direta ou indireta, com o seu titular.

2.4 – Pseudonimização

Tratamento por meio do qual o dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

2.5 – Encarregado pelo Tratamento de Dados Pessoas (Data Protection Officer – DPO)

Pessoa indicada pelo Hospital São Mateus para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD).

2.6 – Tratamento de Dados

Toda operação realizada com dados pessoais; como as que se referem a: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, armazenamento, processamento, arquivamento, eliminação, avaliação ou controle de informação, modificação, transferência, difusão ou extração.

2.7 – Controlador dos Dados

Pessoa natural ou jurídica, de direito público ou privado, a quem competem às decisões referentes ao tratamento de dados pessoais.

2.8 – Operador de Dados

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

2.9 – Banco de Dados

Conjunto estruturado de dados que se relacionam entre si de forma a criar algum sentido (informação).

2.10 – Titular dos Dados

Pessoal natural a quem se refere os dados pessoais que são objeto de tratamento.

2.11 – Minimização dos Dados.

Dados devem ser adequados, relevantes e limitados ao que for necessário em relação as finalidades para as quais são processados.

2.12 – Proporcionalidade

Dados devem ser adequados, relevantes e não excessivos.

2.12 – Subsidiariedade

Dados pessoais só podem ser processados se não houver outros meios para atingir a finalidade.

3 – Descrição

3.1 – Tratamento de Dados

O Hospital São Mateus é o controlador de dados pessoais, coletamos e promovemos o tratamento de dados pessoais de nossos clientes/pacientes para atendimento das finalidades informadas nessa política, utilizando princípio da minimização dos dados, proporcionalidade e subsidiariedade.

3.2 – Dados Coletados

Durante a vigência da relação entre as partes e para fins do cumprimento da prestação de serviços, bem como para melhorias do atendimento, poderão ser coletados dados pessoais, conforme necessário.

3.3 – Coleta de Dados pessoais

Os dados pessoais são coletados a partir do primeiro atendimento na recepção, seja para atendimento ambulatorial, pronto socorro ou internação, a coleta é realizada baseada em interesses legítimos e não menosprezam seus interesses relacionados à proteção de dados pessoais ou liberdades e direitos fundamentais.
Após a primeira coleta, com o decorrer da prestação de serviço, dados pessoais sensíveis irão ser gerados em nossa base de dados, como resultados de exames, evoluções da enfermagem, evoluções médicas, prescrições dentre outros, tais dados estarão armazenados de forma segura e seguindo todos os princípios da proteção de dados pessoais citados nessa política.

3.4 – Tipo de Dados

Tipo de Dados	Dados Pessoais	Finalidade do Uso de Dados
Cadastrais – Identificados e Identificáveis	• **Nome Completo** • **Nome da Mãe** • **Telefone** • **Nº Matrícula no Convênio (Carteirinha)** • **RG** • **CPF** • **CPF de Terceiros (caso menor de idade)**	• **Identificar o paciente** • **Cumprir obrigação legal** • **Proteção ao crédito e procedimentos de cobrança**

	• **Endereço**	• **Garantir a segurança do cliente/paciente**
Dados Sensíveis	• **Resultados de Exames** • **Evoluções de Enfermagem** • **Evoluções Médicas** • **Prescrições**	• **Realizar o tratamento do paciente** • **Cumprir obrigação legal** • **Garantir a segurança do paciente**

3.5 – Como utilizamos as informações

- Realização do tratamento do cliente/paciente
- Fornecer acesso a resultados de exames
- Verificar a identidade do cliente/paciente
- Comunicar com o cliente/paciente e familiares
- Processar transações financeiras

3.6 – Compartilhamento

O Hospital informa que compartilha os dados pessoais com as operadoras de saúde para o atendimento das finalidades informadas nessa política, tendo ainda que compartilhar com autoridades dentro das hipóteses de cumprimento de obrigação legal ou regulatória, administração pública, cumprimento de contrato, realização de estudos por órgão de pesquisa. O Hospital São Mateus irá compartilhar o mínimo de informação necessária para atingir as finalidades, seguindo os princípios de minimização dos dados, proporcionalidade e subsidiariedade e sempre que possível a anonimização dos dados.

3.7 – Contratação

O Hospital São Mateus poderá contratar serviços de processamento e armazenamento de dados (operador), de forma que o cliente/paciente esteja ciente sobre o acesso e tratamento de seus dados por terceiros, cuja a contratação é respaldada por um contrato em conformidade com a Lei Geral de Proteção de Dados e tenha por objetivo garantir a confidencialidade, disponibilidade, integridade dos dados.

3.8 – Segurança dos Dados

O Hospital São Mateus faz uso das melhores práticas de segurança da informação, aplicando medidas técnicas e administrativas para a proteção de dado pessoal, exigindo de seus parceiros o mesmo nível aceitável de segurança da informação.

3.9 – Servidores de Armazenamento

Os dados coletados são armazenados em servidores próprios do Hospital São Mateus, localizados no CPD da instituição e com backups armazenados em Data Center fora do território nacional, cumprindo disposições sobre transferência internacional de dados, conforme artigo 33 da Lei Geral de Proteção de Dados.

3.10 – Retificação, Portabilidade e Exclusão dos Dados.

O cliente/paciente poderá solicitar, a qualquer momento, a ratificação, portabilidade e exclusão de seus dados pessoais.

3.11 – Alteração do consentimento

O cliente/paciente poderá alterar sua concessão de consentimento, conceder novas permissões e retirar seu consentimento em qualquer momento, sendo comunicado das conseqüências que a retirada poderá causar.

3.12 – Acesso à Base de Dados

O acesso aos dados tratados é restrito apenas a profissionais autorizados, tendo possibilidade de auditoria em qualquer alteração na base de dados.
O uso, acesso e compartilhamento, quando necessários, estarão de acordo com as finalidades descritas nessa política.

4 – Armazenamento e Registro de Dados Pessoais

4.1 – Armazenamento de Dados

Dados Cadastrais e de Identificação	
Prazo de Armazenamento	**Fundamento Legal**
5 anos após o término da relação	Art. 12 e 34 do código de defesa do consumidor
Dados Sensíveis (Prontuário Médico) físico e digital	
20 anos após o último registro	Art. 6 Lei n° 13.787/18
Outros dados	
Enquanto durar a relação e não houver pedido de apagamento ou revogação de consentimento	Art. 9 Inciso II da Lei Geral de Proteção de Dados 13.709/2018

4.2 – Exclusão dos Dados

Os dados poderão ser apagados antes desse prazo, caso solicitado pelo titular dos dados, no entanto, pode ocorrer de alguns dados precisarem ser mantidos, nos termos do artigo 16 da Lei Geral de Proteção de Dados, para cumprimento de obrigação legal ou regulatória.

4.3 – Direitos Básicos

O cliente/paciente poderá solicitar ao Encarregado de Dados Pessoais (DPO) a confirmação da existência do tratamento de Dados Pessoais, além do acesso e/ou retificação de seus Dados Pessoais por meio de nosso canal de atendimento.

4.4 – Limitação, Oposição e Exclusão dos dados

O cliente/paciente poderá solicitar a qualquer momento pelo nosso canal de atendimento:

- Limitação ou anonimização do uso de seus Dados Pessoais;
- Revogar o consentimento quanto ao uso de seus Dados Pessoais;
- Solicitar a exclusão de seus Dados Pessoais desde que o Dado Pessoal não faça parte do cumprimento de obrigação legal;
- Solicitar a portabilidade de seus Dados Pessoais para outro prestador de serviços da área da saúde, mediante a requisição expressa, de acordo com a regulamentação da autoridade nacional de proteção de dados (ANPD);

5 – Relatório de impacto à proteção de dados pessoais (DPIA/RIPD)

Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais dos titulares dos dados pessoais, bem como medidas, salvaguardas e mecanismos de mitigação de riscos.

5.1 – Violação

Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos do Hospital São Mateus.

5.2 – Violação de dados pessoais

Ocorre quando de alguma forma dados pessoais são acessados por pessoas ou entidades não autorizadas, podendo ocasionar a destruição, perda, alteração, divulgação acidental ou ilegal dos dados pessoais.

6 – Descrição

6.1 – Diretrizes Gerais

6.1.1 – Princípios do tratamento de dados.

a) Adequação: Compatibilidade do tratamento com as finalidades ao titular, de acordo com o contexto do tratamento. O tratamento de dados deverá ser condizente à destinação à qual se refere, não apresentando-se de forma contraditória à finalidade destinada. A coleta de dados deverá ser compatível com a atividade fim do tratamento, não podendo apresentar uma relação destoante entre o titular dos dados e o controlador.

b) Necessidade: A coleta de dados deve ser sempre restritiva, prezando pelo tratamento de dados pessoais e estritamente necessários ao atendimento da finalidade pretendida, dispensando a coleta excessiva.

c) Transparência: Visa oferecer garantia aos titulares dos dados, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, bem como formulada numa linguagem clara e simples que se recorra adicionalmente à visualização sempre que for adequado.

d) Livre acesso: Como citado no princípio da transparência que exige que as informações e comunicações relacionadas ao tratamento de dados sejam de fácil acesso e compreensão,

formuladas em linguagem clara e simples, consequentemente o titular dos dados tem o livre acesso para consultar, de forma facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

e) Qualidade dos dados: Partindo no mesmo sentido dos princípios da transparência e do livre acesso, o princípio da qualidade dos dados garante aos titulares exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. Como vimos na própria Lei Geral de Proteção de Dados, Lei N° 13709/2018, o titular dos dados tem o direito de correção de dados incompletos, inexatos ou desatualizados e ainda informações das entidades públicas e privadas com as quais o controlador realizou o uso compartilhado de dados e sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

f) Segurança: Compreende nas medidas técnicas e organizacionais aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Atua junto ao princípio da prevenção, utilizando mecanismos para mitigar e poder prevenir de eventuais incidentes.

g) Prevenção: A prevenção está relacionada diretamente aos três pilares da segurança da informação (disponibilidade, integridade e confidencialidade), onde é necessário se precaver de eventuais ameaças, adotando medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

h) Responsabilização e prestação de contas: Dispõe que o agente de tratamento de dados pessoais, deverá demonstrar todas as medidas eficazes e capazes de comprovar o cumprimento da LGPD e eficácia nas medidas aplicadas.

i) Não discriminação: O tratamento de dados não pode ser realizado para fins discriminatórios ilícitos ou abusivos.

j) Finalidade: Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

6.2 – Ciclo de vida do dado pessoal

6.2.1 – Coleta

A coleta do dado pessoal significa a entrada do dado pessoal no Hospital São Mateus, podendo ser por meio de sistemas de informação ligados a software ERP, aplicativos, recebimentos de arquivos, troca de mensagens por e-mail ou por telefone, bem com no ambiente físico como preenchimentos de formulários.

a) **Transparência:** Antes de realizar o tratamento de dados pessoais, o titular dos dados deve receber informação clara e concisa, de fácil acesso e compreensão sobre a coleta, finalidade, armazenamento, compartilhamento e descarte de seus dados. Para o Hospital São Mateus realizar o tratamento dos dados pessoais, devem ser apresentadas, no mínimo as seguintes informações:

- O canal de contato com o encarregado pelo tratamento de dados pessoais no Hospital São Mateus;

- As finalidades específicas e forma de tratamento dos dados;
- A qualificação do Hospital São Mateus como agente de tratamento (controlador ou operador) e seus dados de contatos.
- O tempo de retenção dos dados pessoais, levando em consideração a finalidade do tratamento (deve estar de acordo com a lei de armazenamento de dados de prontuário médico);
- Demais agentes de tratamento com os quais o Hospital São Mateus realiza o uso compartilhado de dados pessoais, tanto entidades públicas como privadas;
- Se o tratamento dos dados pessoais se baseia em interesse legítimo do Hospital São Mateus ou com terceiros.
- Se ocorrer transferência de dados pessoais para outro país, por meio de armazenamento em nuvem em que o Data Center esteja localizado em outro país.
- Quando o consentimento do titular dos dados pessoais for necessário, dispor acerca da possibilidade do não consentimento e as consequências que a negativa pode ocasionar, bem como possibilitar que o titular dos dados revogue o consentimento nos termos da lei aplicável.
- Os direitos do titular dos dados pessoais, confirmação da existência do tratamento, acesso aos dados pessoais, correção de dados pessoais incompletos, inexatos ou desatualizados, portabilidade de dados pessoais, bloqueio ou eliminação de dados pessoais desnecessários, excessivos ou tratados em desconformidade com a legislação aplicável;
- Os riscos, regras e garantias associadas ao tratamento dos dados pessoais, os meios que o titular destes dados dispões para exercer seus direitos relativamente a esse tratamento;

b) **Proporcionalidade:** Deve ser tratado o menor volume de dados pessoais possível, levando em conta que o volume deve ser proporcional aos objetivos do negócio;

c) **Minimização:** Os dados pessoais devem ser limitados ao mínimo necessário para execução das finalidades. Não podendo realizar a coleta de dados sem uma finalidade definida;

d) **Subsidiariedade:** Os dados pessoais devem ser coletados e tratados somente se não existir outro meio para execução do processo

e) **Limitação e armazenamento:** Os dados pessoais devem ser armazenados por um período limitado, exceto quando o agente de tratamento tiver obrigação legal baseado em leis de ter que armazenar esses dados por um longo período, (ex: Prontuário Médico).

f) **Licitude:** O princípio da licitude se relaciona com as 10 bases legais para o tratamento de dados pessoais presentes na lei 13.709/2018.

Abaixo temos a divisão da tabela da seguinte forma:

Hipótese de tratamento de dados: são as situações que autorizam o tratamento de dados pessoais;
Definição: corresponde à característica determinante em relação às bases legais da LGPD.

Base Legal: em nossa tabela, nos referimos à base legal com o dispositivo específico no qual constam as hipóteses de tratamento de dados em íntegra.

Hipótese de tratamento de dados	Definição	Base Legal
Consentimento do titular	Consentimento para tratamento dos dados pessoais deverá ser livre e inequívoco.	Art. 7, I, LGPD
Cumprimento de obrigação legal ou regulatória	Pode ocorrer por força de lei anterior ou para garantir a ordem e segurança social.	Art. 7, II, LGPD
Uso compartilhado de dados pela administração pública	Feito com a finalidade específica de execução de política pública formalmente instituída por Lei ou Ato administrativo.	Art. 7, III, LGPD
Realização de estudos de pesquisa	Tratamento para pesquisar ou estudos para saúde pública ou programa de governo.	Art. 7, IV, LGPD
Execução ou preparação de contrato	Fazer parte de contrato demonstrando consentimento específico do titular para utilização dos dados na execução ou na preparação de negócio jurídico em que seja parte.	Art. 7, V, LGPD
Exercício de direitos em processo judicial, administrativo ou arbitral	Previsão para exercício regular de direito, incluindo contraditório, ampla defesa e devido processo legal.	Art. 7, VI, LGPD
Proteção da vida ou da incolumidade física	Tratamento de dados em favor do titular do dado em casos de necessidade de tutela do bem maior da pessoa natural.	Art. 7, VII, LGPD
Tutela da saúde do titular	Única hipótese de tratamento de dado manejado por agente exclusivo: profissionais de saúde, serviços de saúde ou autoridade sanitária.	Art. 7, VIII, LGPD
Legítimo interesse	Previsão geral e subsidiária, mediante prévia e expressa motivação pelo controlador da finalidade e necessidade (legítimo interesse) do tratamento.	Art. 7, IX, LGPD
Proteção do crédito	Tratamento para proteção e manutenção do crédito.	Art. 7, X, LGPD

g) **Consentimento:** O consentimento do titular dos dados deve ocorrer de vontade livre, pode ser dado de modo escrito, digital ou oral, sendo fundamental que o Hospital São Mateus registre e comprove o consentimento do titular. Para tratamento de dados pessoais sensíveis deve ser possível de ser coletado de forma específica e destacada, para finalidades específicas.

h) **Consentimento de menores de idade:** O tratamento de dados pessoais de menores de idade deve ocorrer somente se o consentimento for dado por pelo menos um dos pais ou pelo responsável legal.

6.2.2 – Armazenamento

O armazenamento dos dados pessoais pode ser realizado de modo físico (cartões, fichas cadastrais, papéis com anotações a mão, formulários, notas fiscais, contratos, prontuários impressos dentre outros) ou digital (mídias como cd, DVD, blueray, disco rígido, disco sólido, pendrives, cartão de memória, serviços de armazenamento em nuvem).

Quando o titular dos dados pessoais solicitar a correção ou atualização de seus dados pessoais, o encarregado pelo tratamento de dados pessoais (DPO), deve analisar a requisição e em seguida acionar as áreas responsáveis para assegurar que os meios físicos e digitais onde esses dados pessoais foram replicados e armazenados sejam também atualizados.

6.2.3 – Uso

O uso dos dados pessoais deve ser realizado sempre dentro dos limites das finalidades legítimas informadas na coleta, caso haja necessidade de realizar o tratamento para outra finalidade é necessário verificar alguns pontos.

- **a)** Qualquer ligação entre a finalidade para a qual os dados pessoais foram coletados e a finalidade do novo tratamento;
- **b)** Relação entre o titular dos dados e o Hospital São Mateus;
- **c)** Se os dados pessoais coletados estão sendo compartilhados com outros agentes de tratamento;
- **d)** Se há dados pessoais sensíveis envolvidos;
- **e)** As consequências do novo tratamento para o titular dos dados;
- **f)** A existência de medidas de segurança adequadas, como anonimização;

Tais informações devem ser encaminhadas ao encarregado pelo tratamento de dados pessoais (DPO) para que este defina se o novo tratamento já está ou não legitimado, caso não esteja, deve propor as estratégias de como este tratamento pode ser legitimado antes de ser realizado. Levando sempre em consideração que o titular dos dados deve ser informado do novo tratamento de dados antes do mesmo realizado, o legítimo interesse deve ser previamente analisa pelo DPO.

6.2.4 – Compartilhamento

Compartilhamento de dados pessoais em território nacional pode ser feito para agentes de tratamentos autorizados, com as medidas de segurança indicadas pelo setor de gestão de segurança da informação a partir do relatório de impacto sobre a proteção de dados pessoais (DPIA/RIPD), esse compartilhamento só pode ser feito para as finalidades do uso previamente informadas e legitimadas junto ao titular dos dados.

O compartilhamento de dados pessoais com demais agentes de tratamento, somente poderá ocorrer caso estes tenham firmado contrato com cláusulas referentes à proteção de dados pessoais.

O compartilhamento de dados pessoais somente poderá ocorrer com o consentimento do titular dos dados pessoais, sendo que este deve ser coletado antes do início do tratamento dos dados pessoais.

6.2.5 – Transferência internacional de dados pessoais

Caso os dados pessoais tenham a previsão de serem transferidos para outro país, a possibilidade de compartilhamento com outro agente de tratamento deverá ser submetida à análise do encarregado pelo tratamento de dados pessoais (DPO), pela área de gestão de segurança da informação e a área jurídica, de modo que todos possam avaliar se o país de destino possui grau de proteção de dados que esteja adequado ao ordenamento jurídico brasileiro.

Caso o agente de tratamento receptor oferecer e comprovar garantias de cumprimento dos direitos do titular, a transferência internacional de dados também poderá ser possível na forma de, cláusulas contratuais específicas para determinada transferência, cláusulas contratuais padrões, normas corporativas globais e selos, certificados e códigos de conduta emitidos pela Autoridade de Proteção de Dados.

Outras formas de ocorrer transferências internacionais de dados pessoais são a partir das finalidades abaixo:

a) Quando a transferência for necessária para a proteção da vida do titular ou de terceiros;
b) Quando a Autoridade Nacional autorizar a transferência;
c) Quando a transferência resultar em compromisso assumido em acordo de cooperação;
d) Quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente está de outras finalidades;
e) Para cumprimento de obrigação legal ou regulatória pelo Hospital São Mateus;
f) Quando necessária para execução de contrato e procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

6.2.6 – Eliminação dos dados pessoais

a) Os dados pessoais devem ser armazenados por período limitado, levando em consideração a finalidade específica do tratamento;
b) Após exercida a finalidade do tratamento e fim do prazo de armazenamento determinado por obrigação legal, os dados podem ser eliminados de modo seguro, sejam eles registrados em meios físicos ou digitais.;
c) A eliminação dos dados pessoais poderá ser realizada também a pedido do titular do dado ou da Autoridade Nacional de Proteção de Dados;
d) Para eliminação dos dados devem ser seguidas as definições indicadas no procedimento de eliminação de dados segura;
e) A conservação dos dados pessoais após atingida a finalidade só será possível no caso de cumprimento de obrigação legal;
f) A solicitação de eliminação do dado pessoal pelo titular não será possível quando o dado já ter sido anonimizado;
g) A solicitação de eliminação por parte do titular não poderá ser realizada no caso de cumprimento de obrigação legal quanto ao armazenamento destes dados para fins regulatórios.

7 – Resposta à requisição do titular dos dados pessoais

Os procedimentos de resposta às requisições dos titulares dos dados pessoais serão regidos pelo protocolo de resposta à requisição do titular dos dados pessoais, disponível na base de documentação do Hospital São Mateus.

Todos os colaboradores e prestadores de serviço do Hospital São Mateus têm o dever de notificar o encarregado pelo tratamento de dados pessoais (DPO), sem demora injustificada,

sobre qualquer requisição recebida do titular dos dados pessoais antes de responder a requisição, sempre buscando orientação sobre as melhores práticas de comunicação a ser estabelecida com o titular dos dados pessoais.

Qualquer existência de dúvida e/ou situações específicas, o colaborador ou prestador deve encaminhar a requisição ao encarregado pelo tratamento de dados pessoais (DPO), para que o mesmo responda de forma mais adequada perante a legislação específica aplicável e às boas práticas estabelecidas internamente ou vistas no mercado.

7.1 – Acesso aos dados pessoais pelo titular dos dados

O titular dos dados pessoais pode requerer a qualquer momento o acesso aos seus dados pessoais, devendo o colaborador e/ou prestador de serviço da área responsável pelo tratamento assegurar que a identidade do titular dos dados pessoais seja comprovada conforme procedimento de reposta à requisição do titular dos dados pessoais.

A requisição e posteriormente acesso aos dados pessoais devem ocorrer, preferencialmente, de modo eletrônico, exceto quando o titular dos dados pessoais expressamente requerer o envio dos dados pessoais de modo físico ou divulgação de modo oral.

7.2 – Eliminação e/ou bloqueio de tratamento dos dados pessoais por requisição do titular dos dados pessoais

O titular dos dados pessoais pode requerer a qualquer momento a eliminação e/ou bloqueio do tratamento de seus dados pessoais, devendo o colaborador ou prestador de serviço da área responsável pelo tratamento encaminhar a requisição de eliminação/bloqueio ao encarregado pelo tratamento de dados pessoais para que possam ser adotadas as medidas necessárias conforme indicado no procedimento de resposta à requisição do titular dos dados pessoais.

Na impossibilidade de eliminação dos dados, o titular deve ser informado sobre esta decisão, explicando os motivos pelos quais estes dados pessoais não poderão ser apagados.

7.3 – Resposta a ANPD (Agencia Nacional de Proteção de Dados)

Os colaboradores ou prestadores de serviço têm o dever de notificar o encarregado pelo tratamento de dados pessoais e a área jurídica do Hospital São Mateus, sem demora injustificada e antes de responder à Autoridade, sobre qualquer ordem ou requisição relativa à privacidade e proteção de dados pessoais recebida da ANPD (Agência Nacional de Proteção de Dados).

7.4 – Resposta a autoridade judicial

Os colaboradores ou prestadores de serviço devem notificar imediatamente o encarregado pelo tratamento de dados pessoais (DPO) e o jurídico do Hospital São Mateus sobre qualquer ordem ou determinação judicial relativa a dados pessoais de que tome conhecimento.

Quando requisitado por meio de ordem judicial, caberá ao jurídico fornecer esclarecimentos e entregar as informações demandadas pela autoridade, sem demora injustificada, podendo requisitar o apoio do encarregado de proteção de dados pessoais (DPO).

Quando a autoridade determinar a necessidade de prestação de esclarecimentos, será responsabilidade do jurídico do Hospital São Mateus buscar informações e esclarecimentos junto ao encarregado pelo tratamento de dados pessoais, colaboradores e/ou prestadores de

serviço que tenham envolvimento no fluxo de dados pessoais, de forma a coletar o máximo de informações pertinentes para estruturar uma resposta adequada.

7.5 – Violação de dados pessoais

O setor de segurança da informação deve implementar controles técnicos capacitando o Hospital São Mateus a evitar possíveis violações de dados em seu ambiente lógico e se ocorrerem, possibilitar reportar estas em tempo hábil à ANPD (Agência Nacional de Proteção de Dados).

Os colaboradores e/ou prestadores de serviço têm a obrigação de notificar a área de gestão de segurança da informação, sem demora injustificada, acerca de qualquer violação ou tentativa de violação de dados pessoais da qual tenham conhecimento.

Todos colaboradores e/ou prestadores de serviço devem na medida do possível, cooperar para investigação e mitigação de incidentes de violação de dados pessoais.

Todos os procedimentos realizados nesta seção devem ser documentados pelas partes envolvidas, sob a supervisão do encarregado pelo tratamento de dados pessoais (DPO).

7.6 – Segurança da Informação

Durante o ciclo de vida do dado pessoal sempre devem ser observados as diretrizes de segurança da informação existentes na Política de Segurança da Informação e na Política de Privacidade de Dados Pessoais do Hospital São Mateus.

O setor de gestão de segurança da informação deve assegurar os 3 pilares da segurança da informação, que são a disponibilidade, integridade e confidencialidade do dado pessoal em todos os meios de armazenamento e transmissão.

a) Controles técnicos de segurança da informação:
    - Firewall;
    - Criptografia;
    - Utilização de VPN (Virtual Private Network) para acesso externo aos dados do Hospital São Mateus;
    - Controles de acesso físicos e lógicos;
    - Autenticação de dois fatores;
    - Armazenamento seguro de documentos físicos;
    - Políticas de senhas.

b) Assegurar que somente pessoas autorizadas e agentes de tratamentos de dados autorizados tenham acesso aos dados pessoais (confidencialidade);
c) Adoção de medidas de segurança da informação para assegurar que os dados pessoais se mantenham íntegros sem alterações indevidas, exatos, completos e atualizados (integridade);
d) Garantia de que os dados pessoais sejam acessíveis e utilizáveis pelas pessoais e entidades autorizadas sempre que sejam necessários (disponibilidade);
e) Registro de logs e trilhas de auditoria do ciclo de vida do dado pessoal
f) Criptografia, pseudonimização e anonimização dos dados pessoais quando for necessário;
g) Medidas organizacionais, treinamento em proteção de dados pessoais e supervisão da adoção das práticas ensinadas.

8 – Disposições Gerais

8.1 – Atualizações dos Termos

O Hospital São Mateus reserva-se ao direito de alterar o conteúdo desta Política a qualquer momento, conforme a necessidade de adequação e conformidade com a Lei Geral de Proteção de Dados ou norma que tenha força jurídica equivalente.

8.2 – Considerações Finais

Esta Política foi criada a partir das estratégias do negócio e com base na lei 13.709/2018 – Lei Geral de Proteção de Dados – LGPD e deve ser revisada no mínimo 1 vez a cada 6 meses ou sempre que houver mudanças significativas na estrutura organizacional.

8.3 – Canais de Atendimento

- **Encarregado pelo Tratamento de Dados Pessoais (DPO):**
  - Daniel Badinhani – encarregado@hsaomateus.org
  - Tel.: (61) 98246-0189 / (61) 3362-0045 / (61) 3030-1795
  - https://www.hsaomateus.org/encarregado