Histórico de Versões e Alterações				
Versão	Data	Responsável	Tipo de Alteração	Revisor/Aprovador
1	20/10/2025	Samuel	Criação da Política	Igo
2	22/10/2025	Ageu	Padronização de termos	Larissa
3	24/10/2025	Samuel	Adição de tópicos	Larissa

Sumário

1. Objetivo e Diretrizes Gerais

O objetivo principal desta política é assegurar que as informações recebam classificação apropriada de confidencialidade, integridade, disponibilidade, autenticidade e privacidade (CIDAP), de acordo com sua sensibilidade e criticidade para o hospital e para os titulares dos dados.

As diretrizes essenciais para o ambiente hospitalar são:

a. **Proteção Mandatória de Dados Sensíveis:** O tratamento de informações deve respeitar a privacidade e a proteção de dados pessoais, especialmente aqueles definidos pela Lei nº 13.709/18 (LGPD), como dados de saúde ou biometria.
b. **Classificação no Ciclo de Vida:** Todas as informações e ativos (documentos digitais, físicos e sistemas) devem ser classificados na sua emissão ou recepção, e revisadas periodicamente para garantir que a classificação permaneça adequada.
c. **Princípio da Necessidade de Conhecimento (Need-to-Know):** O acesso deve ser limitado a pessoas especificamente autorizadas que necessitem da informação para o desempenho de suas tarefas profissionais.

2. Escopo e Responsabilidades

2.1. Abrangência da Política

Esta política é aplicável a todos os ativos de informação (documentos digitais, físicos e sistemas) e a todas as pessoas que, direta ou indiretamente, acessem, tratem ou suportem as informações do hospital. Isto inclui, mas não se limita a: colaboradores (funcionários, médicos, estagiários), gestores e diretores, consultores, fornecedores e terceiros que realizem qualquer tratamento de informações em nome do hospital.

2.2. Papéis e Responsabilidades

A responsabilidade pela classificação correta, manuseio e proteção das informações deve ser atribuída para garantir a rastreabilidade e a conformidade.

a) **Proprietário da Informação (Data Owner):** Normalmente o gestor da área de negócio (ex: Diretor Clínico, Gerente Financeiro) que cria, utiliza ou é responsável pelas informações. É o responsável final pela classificação correta, pela aplicação desta política em suas equipes, e pelo estabelecimento dos critérios de tratamento da informação. O Proprietário da Informação deve garantir que as informações sejam corretamente classificadas e rotuladas.
b) **Custodiante da Informação (Data Custodian/TI):** A equipe responsável pela segurança tecnológica, armazenamento, processamento e manutenção dos sistemas e infraestrutura que suportam a informação. Deve assegurar os recursos tecnológicos e sistemas para o tratamento seguro da informação.
c) **Usuário da Informação (Colaborador):** Qualquer pessoa que acesse ou utilize a informação para o desempenho de suas tarefas profissionais. Deve cumprir rigorosamente as diretrizes de classificação e proteção, e reportar imediatamente quaisquer não conformidades ou eventos de segurança.
d) **Encarregado de Dados (DPO):** Responsável por atuar como canal de comunicação com os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), garantindo que o tratamento dos Dados Pessoais Sensíveis (como prontuários médicos) siga os requisitos legais da Lei Geral de Proteção de Dados (LGPD).

3. Definição dos Níveis de Classificação

A classificação da informação no hospital deve ser realizada de acordo com o nível de impacto potencial em caso de divulgação, modificação ou destruição não autorizada.

Nível de Classificação	Impacto Potencial (Confidencialidade)	Descrição e Critérios de Acesso	Exemplos
PÚBLICA	Muito Baixo	Informação oficialmente liberada para divulgação ampla, sem causar danos ou prejuízos ao hospital. Acesso irrestrito.	Horário de atendimento, lista de especialidades médicas, políticas, relatórios anuais de gestão sem dados sensíveis e campanhas públicas de saúde.
INTERNA	Baixo	Informação destinada ao uso interno do hospital, para usuários e departamentos específicos. Sua divulgação ao público em geral requer autorização expressa e não deve causar problemas significativos.	Manuais de procedimentos operacionais, relatórios gerenciais internos (sem dados de pacientes), lista de ramais, e-mails corporativos, comunicados internos e avisos gerais.
RESTRITA	Moderado	Informação cujo acesso é limitado a grupos específicos de colaboradores. A divulgação não autorizada pode prejudicar investigações em	Documentos internos de tomada de decisão, relatórios de auditoria interna (não sensíveis), relatórios

		andamento ou comprometer atividades administrativas sensíveis.	financeiros internos e planejamentos administrativos.
CONFIDENCIAL	Alto/Muito Alto	Informação de caráter sigiloso, cuja divulgação ou alteração não autorizada pode causar graves danos, prejuízos irreversíveis ou violação da lei para o hospital e/ou terceiros. Este nível é obrigatório para Dados Pessoais Sensíveis.	Prontuários médicos de pacientes, resultados de exames, histórico de internações, dados biométricos, informações salariais e contratuais de colaboradores, segredos comerciais ou propriedade intelectual (ex: pesquisa clínica confidencial).

3.1. Classificação Padrão (Omissão de Rótulo)

Caso um documento ou ativo de informação não contenha um rótulo de classificação visível ou a rotulagem não seja tecnicamente possível (restrições de sistema), a informação deve ser tratada por padrão como INTERNA. Se houver qualquer dúvida quanto à presença de Dados Pessoais Sensíveis ou criticidade moderada, o tratamento deverá ser o mais restritivo possível, sendo elevada para, no mínimo, RESTRITA até que o Proprietário da Informação defina o nível correto.

3.2. Revisão e Análise Crítica das Classificações

Todas as informações e ativos devem ter sua classificação revisada periodicamente para garantir que o nível atribuído permaneça adequado. O

processo de análise crítica da classificação deve ser realizado a cada 12 meses (anualmente), ou sempre que ocorrerem mudanças relevantes, como:

a) Mudanças nos critérios de classificação ou na legislação (ex: LGPD).
b) Mudanças nas necessidades do negócio ou na sensibilidade da informação.
c) Ocorrência de eventos ou incidentes de segurança.
d) Ao longo do ciclo de vida da informação.

4. Critérios de Tratamento e Manuseio Específicos

O tratamento da informação é o conjunto de ações (produção, classificação, utilização, acesso, armazenamento, eliminação, etc.). Para o hospital, o tratamento deve ser rigorosamente controlado para garantir os princípios de CIDAP.

4.1. Tratamento de Dados Pessoais Sensíveis (Confidencial)

a) **Fundamento Legal:** O tratamento de dados de saúde deve seguir os requisitos legais da LGPD, sendo os dados de saúde classificados como Confidenciais.
b) **Anonimização/Pseudonimização:** Sempre que possível e aplicável à finalidade, as informações devem ser anonimizadas ou pseudonimizadas, reduzindo o impacto em caso de vazamento.
c) **Registro e Rastreabilidade:** Deve-se manter uma cadeia de custódia e registros claros de quem acessou, modificou ou transferiu prontuários e dados de pacientes.

4.2. Diretrizes de Rotulagem

A rotulagem visa comunicar o nível de classificação da informação contida no documento, facilitando seu manuseio e proteção.

a) **Formatos:** Os procedimentos de rotulagem devem abranger todos os formatos: documentos físicos (prontuários, radiografias), documentos digitais (e-mails, sistemas) e informações verbais.
b) **Técnicas Recomendadas:** Para documentos digitais de nível RESTRITA ou CONFIDENCIAL, recomenda-se o uso de cabeçalhos, rodapés ou marcas d'água que indiquem claramente o nível de classificação (Ex: "CONFIDENCIAL – DADOS DE PACIENTE").
c) **Omissão:** Se a rotulagem não for tecnicamente possível (restrições de sistema), o tratamento deve ser o mais restritivo, conforme o nível de classificação presumido.

4.3. Diretrizes para Transferência de Informações

A transferência de informações (entre áreas internas ou com terceiros, como laboratórios externos ou operadoras de saúde) deve ser definida por regras, procedimentos e acordos, alinhados à classificação.

Tipo de Transferência	Requisitos de Controle
Verbal	Não realizar conversas envolvendo dados do tipo CONFIDENCIAL em locais públicos (corredores, elevadores, refeitórios) ou por canais de comunicação inseguros. Em reuniões internas sensíveis, o nível de classificação do assunto deve ser avisado para que todos os presentes observem os controles.
Mídia Física (Prontuários)	As informações do tipo CONFIDENCIAL devem ser transportadas de forma segura. Controles devem proteger contra danos físicos (ex: derramamento de líquidos) e garantir o endereçamento e transporte corretos. Deve-se manter um registro (cadeia de custódia) de quem enviou e recebeu a mídia.
Eletrônica	Informações do tipo CONFIDENCIAL (ex: resultados de exames via e-mail) devem ser

	protegidas contra malware e enviadas com prevenção contra destinos incorretos. Deve-se utilizar criptografia ou canais seguros para transferência de dados sensíveis e autenticação rigorosa ao acessar sistemas remotamente.

4.4. Diretrizes de Retenção e Descarte

O tratamento da informação inclui o conjunto de ações de eliminação, arquivamento e destinação. Devem ser definidas diretrizes de retenção e descarte para todos os registros, em alinhamento com a classificação, a sensibilidade e os requisitos legais (como a LGPD).

O tempo de retenção das informações deve ser baseado em requisitos legais, regulamentares (ex: normas do Conselho Federal de Medicina sobre guarda de prontuários) e contratuais.

O método de descarte deve ser proporcional ao nível de classificação e ao impacto potencial de vazamento.

Nível de Classificação	Requisito de Retenção e Descarte	Método de Descarte
PÚBLICA	Descarte quando não houver valor histórico ou legal.	Eliminação Lógica Padrão (para mídias digitais); Reciclagem (para mídias físicas).
INTERNA	Definido pelo Proprietário da Informação, respeitando o ciclo de vida da informação.	Eliminação Lógica Padrão (para mídias digitais); Descarte seguro que impeça leitura superficial (mídias físicas).
RESTRITA	Retenção conforme determinação legal ou regulatória específica (ex: 5 anos, se	Descarte deve ser rastreável e controlado. Recomenda-se trituração ou

	aplicável a contextos de sigilo legal).	incineração (físico); Eliminação Lógica com verificação de não recuperabilidade (digital).
CONFIDENCIAL	Período de retenção rigoroso, determinado pela legislação de saúde e LGPD.	Deve ser utilizado o método de descarte mais seguro: Trituração física segura (para prontuários e exames impressos) ou Wipe Criptográfico/Sanitização de Mídia (para mídias digitais e discos) que impossibilite a recuperação dos dados, devendo haver registro (log) e cadeia de custódia do processo de descarte.

5. Auditoria e Conformidade

A Equipe de Segurança da Informação do hospital é responsável por monitorar e auditar o cumprimento desta Política, visando avaliar a eficácia e a eficiência dos controles de segurança.

5.1. Manutenção de Evidências

a) A equipe de segurança deve manter registros (logs) e evidências que assegurem a rastreabilidade e não repúdio das ações realizadas sobre informações classificadas.

b) As evidências incluem a manutenção de uma cadeia de custódia de prontuários e dados de pacientes, registros de acesso e modificação, e registros de auditoria e logs de segurança.

c) Devem ser realizadas amostragens periódicas de documentos, mídias e sistemas para verificar a rotulagem e o tratamento.

5.2. Indicadores de Conformidade

O gestor de segurança e o comitê de segurança da informação devem acompanhar indicadores simples para avaliar a eficácia dos controles, como:

a) Percentual de informações/ativos corretamente classificados e rotulados.
b) Número de incidentes de segurança ou vazamentos relacionados à classificação ou rotulagem.
c) Conformidade da retenção e eliminação dos dados CONFIDENCIAIS.
d) Percentual de colaboradores treinados sobre as diretrizes de classificação.

6. Responsabilidades e Penalidades

a) **Proprietários da Informação:** Os gestores de áreas e proprietários de ativos são responsáveis pela correta classificação e garantia da aplicação desta política em suas equipes.
b) **Colaboradores:** Devem seguir as diretrizes de classificação e proteção, reportando imediatamente quaisquer não conformidades ou eventos de segurança.

O não cumprimento desta Política implica em falta grave, podendo resultar em ações disciplinares (advertência, suspensão, rescisão) e/ou processos civis ou criminais, dependendo da natureza e gravidade do vazamento/dano. Para o hospital, a violação de dados do tipo CONFIDENCIAL de pacientes acarreta responsabilidade legal conforme a LGPD.