1. OBJETIVO

Esta Política estabelece as diretrizes para o registro, tratamento e proteção das informações institucionais em todos os setores assistenciais, administrativos e de apoio da Santa Casa, considerando que a qualidade dos registros efetuados é reflexo direto da qualidade da assistência e dos serviços prestados.

2. APLICAÇÃO

Esta política aplica-se a todos os colaboradores, prestadores de serviços, terceiros, estagiários, residentes, corpo clínico e membros da alta gestão que tenham acesso às informações institucionais da Santa Casa.

3. DEFINIÇÕES

Não de aplica.

4. DIRETRIZES

A gestão segura das informações é caracterizada pela atuação integrada de todos os setores da instituição, garantindo que os dados e registros sejam produzidos, utilizados, armazenados, compartilhados e descartados de forma adequada, clara, íntegra, confidencial e rastreável.
As informações institucionais compreendem registros assistenciais, administrativos, financeiros, contábeis, trabalhistas, patrimoniais, tecnológicos e estratégicos, devendo ser tratadas de acordo com sua finalidade, classificação e nível de acesso.
Todos os colaboradores, prestadores de serviços, corpo clínico, estagiários e terceiros autorizados são responsáveis pela proteção das informações sob sua guarda, observando os princípios de confidencialidade, integridade, disponibilidade, autenticidade e conformidade com a legislação vigente, especialmente a Lei Geral de Proteção de Dados (LGPD).
A Santa Casa estabelece mecanismos de controle, monitoramento e segurança para assegurar a qualidade das informações, a continuidade dos processos institucionais e a proteção dos dados de pacientes, colaboradores, fornecedores, parceiros e demais partes interessadas.

4.1 Informação através do registro em prontuário

Todo profissional capacitado e responsável pelas informações para garantir os cuidados dos pacientes na triagem, atendimento e internção devem seguir as diretrizes de segurança abaixo, seja em prontuário eletrônico ou físico.

- Letra legível , dados corretos, sem abreviações do nome do paciente e/ou responsável;
- Não conter rasuras ou corretivos no prontuário do paciente nos casos de documentos físicos;
- Data e horário antes de iniciar o registro da informação;
- Utilizar somente caneta azul ou preta para registro ou assinatura no prontuário do paciente;
- Ser claras, objetivas, legíveis, pontuais e cronológicas;

- Ser precedida de assinatura e identificação (carimbo, quando necessário) do profissional ao final de cada registro/anotação/evolução;
- Não utilizar o termo “paciente”, “cliente” ou “criança” no início de cada frase, tendo em vista, que o prontuário é individual e exclusivo para cada paciente;
- Realizar o registro de modo completo e objetivo, contemplando as impressões técnicas e terapêuticas;
- O registro sobre o estado do paciente deve conter no mínimo: a situação em que o paciente se encontra, breve histórico, avaliação das condições clínicas e recomendações;
- As abreviaturas utilizadas devem ser as padronizadas pela Instituição através de siglário;
- Deixar claro no registro, se a observação foi realizada pelo profissional, pelo paciente ou familiar;
- Não é permitido registrar informações não pertinentes ao paciente, bem como, anotar problemas administrativos;
- Todos os documentos em papel devem conter os marcadores definidos na Política de Identificação do Paciente, como nome completo e data de nascimento.
- Informar ou observar rigorosamente assuntos pertinentes e relevantes que podem trazer riscos ao paciente.
- Marcadores de identificação: uso mandatório de, no mínimo dois identificadores (ex. nome completo e data de nascimento) em todos os pontos de contato (admissão, administração de medicamentos, coletas de exames e terapias);
- Barreiras ativas: uso de pulseiras de identificação com conferência verbal e visual antes de qualquer procedimento. Em sistemas eletrônicos, a confirmação deve ser validada no prontuário antes do registro da assistência;
- Protocolo de lado/sítio: verificaçao dupla em procedimento que envolvam lateralidade ou especificidade de local, prevenindo erros de troca.

4.2 Acesso e controle de informações

A Santa Casa estabelece critérios e procedimentos para controlar o acesso às informações institucionais com base nas atribuições de cada função, necessidades de trabalho e níveis de autorização definidos pela organização. O acesso aos sistemas, documentos físicos, prontuários, registros administrativos e demais informações institucionais é concedido de forma individualizada, mediante mecanismos de segurança como senhas, perfis de acesso, autenticação e monitoramento. O colaborador não poderá retirar, reproduzir, compartilhar ou utilizar ativos de informação da empresa sem autorização expressa da organização. É vedado, ainda, o uso de dispositivos pessoais, mídias removíveis e aplicativos não homologados para tratamento de informações corporativas, bem como a divulgação de dados internos a terceiros não autorizados.

4.3 Retenção e descarte de informações

A Santa Casa estabelece diretrizes para a retenção adequada das informações institucionais, assistenciais, administrativas, financeiras, trabalhistas e demais registros produzidos ou recebidos pela organização, observando os prazos definidos pela legislação vigente, requisitos regulatórios, necessidades operacionais e diretrizes internas.
As informações devem ser mantidas íntegras, acessíveis e protegidas durante todo o seu ciclo de vida, garantindo sua disponibilidade para consultas, auditorias, processos assistenciais e atividades

administrativas quando necessário.
O descarte de informações e documentos físicos ou eletrônicos deverá ocorrer de forma segura, controlada e rastreável, preservando a confidencialidade e evitando acessos não autorizados, vazamentos ou uso indevido de dados.
Os critérios, prazos de retenção e procedimentos para descarte seguro encontram-se detalhados na Política de Retenção e Descarte de Dados da instituição.

4.4 Segurança da Informação

A Santa Casa adota medidas técnicas, administrativas e organizacionais para proteger as informações institucionais contra acessos não autorizados, divulgação indevida, perda, alteração, destruição, vazamento, roubo ou qualquer forma de comprometimento de sua confidencialidade, integridade, disponibilidade e autenticidade.
Para garantir a segurança das informações, a instituição utiliza mecanismos de proteção, tais como controle de acesso por perfil de usuário, senhas individuais, antivírus, firewall, sistemas de monitoramento, backups periódicos, atualização de sistemas, proteção de rede, controle de dispositivos móveis e outras ferramentas de segurança compatíveis com os riscos identificados.
Todos os colaboradores, prestadores de serviços, corpo clínico, estagiários e terceiros autorizados devem utilizar os recursos tecnológicos de forma responsável, observando as diretrizes institucionais de segurança da informação, confidencialidade e proteção de dados.
Qualquer suspeita de incidente de segurança, acesso indevido, perda de informações ou vazamento de dados deverá ser comunicada imediatamente ao gestor responsável e ao setor de Tecnologia da Informação para análise, tratamento e adoção das medidas cabíveis.

4.5 Treinamento e concientização

Estabelecemos que há a necessidade de treinar os profissionais sobre a importância da gestão adequada das informações e a conscientização sobre as práticas recomendadas de segurança e a cada revisão ou novas metodologias do sistema, há reeducação pontual.

4.6 Monitoramento e auditoria

Definimos processos para monitorar regularmente o cumprimento das políticas e procedimentos de gestão de informações. Durante as auditorias internas ou a cada necessidade verificamos, mensuramos e tomamos as devidas ações, se necessário.

4.7 Atualização e revisão

A Política de Gestão de Informações deverá ser revisada periodicamente, ou sempre que houver alterações significativas nos processos institucionais, requisitos legais e regulatórios, tecnologias utilizadas, estrutura organizacional ou necessidades identificadas pela instituição.
As revisões têm como objetivo garantir que as diretrizes permaneçam atualizadas, eficazes e alinhadas às melhores práticas de gestão da informação, segurança da informação, proteção de dados pessoais, requisitos de qualidade e estratégias institucionais.

4.8 Backup seguro (segurança das informações)

O backup do sistema interno é realizado diariamente. O servidor é físico em cada unidade e o backup fica disponível na nuvem.
O fornecedor responsável pelo backup do prontuário eletrônico é o responsável é responsável por comprovar a efetividade das medidas de segurança adotadas. Sempre que houver necessidade de recuperação de dados, esta será solicitada por profissional previamente definido, e a empresa contratada deverá evidenciar o resgate das informações.
Semestralmente solicitamos à empresa contratada levantamento de algum dado ou prontuário de paciente, a fim de comprovar, por meio de simulações, a eficácia da recuperação dos dados quando necessário.

4.9 Pontos de atenção

O paciente, ou seu responsável legal, tem direito de acesso aos registros constantes em seu prontuário, respeitados os limites éticos, legais e institucionais aplicáveis. As informações clínicas devem permanecer restritas ao próprio paciente, aos profissionais diretamente envolvidos na assistência e às pessoas legalmente autorizadas ou expressamente consentidas pelo titular, em conformidade com as normas de sigilo profissional e proteção de dados pessoais (CONSELHO FEDERAL DE MEDICINA, 2002; CONSELHO REGIONAL DE MEDICINA DO DISTRITO FEDERAL, 2022; BRASIL, 2018).
As interações verbais, telefônicas ou por aplicativos de mensagens, inclusive WhatsApp, poderão ser utilizadas apenas para fins assistenciais, de orientação e de acompanhamento terapêutico com pais ou responsáveis, desde que previamente autorizadas e formalizadas em termo interno de conduta, contemplando o dever de sigilo, confidencialidade e proteção das informações (CONSELHO FEDERAL DE MEDICINA, 2002; CONSELHO FEDERAL DE MEDICINA, 2000).
O prontuário deverá conter, de forma legível, cronológica e rastreável, no mínimo: identificação do paciente com pelo menos dois marcadores, como nome completo e data de nascimento; anamnese, ficha ou questionário de admissão; plano e planejamento terapêutico; evolução terapêutica diária ou sempre que necessário; termos de consentimento assinados; e resumo de alta com os registros pertinentes à continuidade do cuidado (CONSELHO REGIONAL DE MEDICINA DO DISTRITO FEDERAL, 2022; CONSELHO FEDERAL DE MEDICINA, 2002).
As anotações devem ser claras, completas e identificáveis, com a devida responsabilização técnica do profissional que as produziu, de modo a assegurar a integridade documental e a segurança assistencial (CONSELHO FEDERAL DE MEDICINA, 2002; BRASIL, 2018).

4.10 Uso de inteligência artificial (IA)

As ferramentas de Inteligência Artificial (IA) generativas ou preditivas podem ser utilizadas pelos colaboradores apenas como suporte a atividades administrativas, operacionais, organização de fluxos de trabalho e auxílio à redação geral, desde que cumpridos os seguintes critérios obrigatórios de segurança:

- Vedação Absoluta de Dados Identificáveis: É terminantemente proibido inserir, colar, digitar ou fazer o upload de qualquer tipo de dado pessoal ou dado pessoal sensível (como nomes de pacientes, números de prontuário, registros gerais, CPFs, históricos clínicos, relatórios assistenciais, exames ou dados funcionais de colaboradores) em ferramentas públicas e gratuitas de IA de terceiros (ex: ChatGPT, Gemini público, Copilot público, etc.).
- Anonimização Mandatória: Caso o profissional necessite de suporte de IA para estruturar

textos, resumos ou minutas administrativas, o texto de entrada (prompt) deve ser submetido a uma rigorosa e completa anonimização prévia, eliminando qualquer fragmento que possa rastrear ou identificar direta ou indiretamente o paciente ou o colaborador.

- Responsabilidade Técnico-Profissional (Validação Humana): Nenhuma decisão clínica, diagnóstico médico, prescrição, planejamento terapêutico ou documento institucional oficial pode ser fundamentado ou gerado de forma exclusiva por IA. Todo conteúdo produzido com auxílio de sistemas de inteligência artificial deve passar por detalhada revisão crítica, correção e validação de um profissional humano capacitado, que responderá civil, ética e administrativamente pela precisão das informações registradas.
- Homologação de Ferramentas: O uso de qualquer software, plataforma, extensão de navegador ou solução tecnológica baseada em IA no ecossistema da instituição depende obrigatoriamente de análise técnica de risco prévia e homologação expressa por parte do setor de Tecnologia da Informação (TI) e do Comitê de Proteção de Dados/DPO da Santa Casa.

5. REFERÊNCIAS

CONSELHO FEDERAL DE MEDICINA. Resolução CFM nº 1.605, de 15 de setembro de 2000. Disciplina o fornecimento de cópia de prontuário médico. Brasília, DF: CFM, 2000.

CONSELHO FEDERAL DE MEDICINA. Resolução CFM nº 1.639, de 10 de julho de 2002. Aprova as normas técnicas para o uso de sistemas informatizados para a guarda e manuseio do prontuário médico. Brasília, DF: CFM, 2002.

CONSELHO REGIONAL DE MEDICINA DO DISTRITO FEDERAL. Manual LGPD CRM-DF. Brasília, 2022.
ORGANIZAÇÃO NACIONAL DE ACREDITAÇÃO. Manual ONA 2022/2025: diretrizes internas. São Paulo: ONA, 2022.

CONSELHO FEDERAL DE MEDICINA. Resolução CFM nº 2.217, de 27 de setembro de 2018. Brasília, DF: CFM, 2018.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 24 jun. 2026.BRASIL. Ministério da Saúde. Ministério da Saúde. Brasília, DF: Ministério da Saúde, s.d

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/*ato2015-2018/2018/lei/l13709.htm*. Acesso em: 24 jun. 2026.planalto.gov

BRASIL. Tratamento de Dados Pessoais - LGPD. Portal Gov.br. Disponível em: https://www.gov.br/planejamento/pt-br/acesso-a-informacao/tratamento-de-dados-pessoais. Acesso em: 24 jun. 2026.gov

6. HISTÓRICO DAS ALTERAÇÕES

VERSÃO	ITEM	NATUREZA DAS ALTERAÇÕES
00 14/11/2024	-	Criação do documento
01 13/04/2026	-	Revisão do documento
02 25/06/2026		

7. ELABORAÇÃO E APROVAÇÃO

ELABORAÇÃO: 14/11/2024	**APROVAÇÃO:** 14/11/2024
ASSINADO DIGITALMENTE POR Wesley Uilquer Santos Dias CPF: 093.100.356-33 Data: 03/07/2026 15:37 -03:00 Wesey Uilquer Santos Dias	Documento assinado digitalmente NATALY LOURDES FONSECA CAMPIDELI ANDRA Data: 10/07/2026 10:36:31-0300 Verifique em https://validar.iti.gov.br Núcleo da Qualidade