CARTILHA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD:

Diretrizes práticas do Hospital de Clínicas de Itajubá

2024

HCI
HOSPITAL DE CLÍNICAS DE ITAJUBÁ-MG
Excelência em Cuidar

PALAVRA DO PRESIDENTE

É com grande satisfação e responsabilidade que apresento nossa cartilha sobre a Lei Geral de Proteção de Dados (LGPD) e as diretrizes aplicadas ao Hospital de Clínicas de Itajubá - HCI. Este documento representa um passo significativo da nova gestão e jornada em conformidade com a legislação que rege a proteção de dados pessoais.

Expresso meus mais sinceros agradecimentos a todos que contribuíram para a elaboração desta cartilha. A dedicação e o empenho da equipe, bem como a colaboração de especialistas na área, foram essenciais para a criação deste material. Agradeço também aos profissionais que, com sua experiência e conhecimento prático, forneceram insights valiosos para que pudéssemos abordar de maneira eficaz as nuances da LGPD no contexto hospitalar.

A proteção de dados não é apenas uma obrigação legal, mas uma questão de respeito e compromisso com a privacidade dos nossos pacientes garantindo a confiança e a integridade dos nossos serviços. Este documento visa fornecer diretrizes claras e práticas para que todos nós possamos operar dentro dos parâmetros estabelecidos pela lei.

À medida que avançamos, encorajo cada um de vocês a abraçar este desafio com espírito colaborativo e proativo. A adaptação a novos procedimentos pode parecer complexa no início, mas é um investimento vital para a qualidade e a segurança do serviço que ofertamos. Lembremos que o sucesso é alcançado através da conscientização contínua, da educação e do engajamento de todos.

Estou confiante de que, juntos, conseguiremos transformar este desafio em uma oportunidade para fortalecer a nossa instituição e a confiança que a sociedade deposita em nós. Agradeço a todos pela dedicação e pelo compromisso com a excelência em nosso ambiente hospitalar.

Carlos Magno Castro Gonçalves
Presidente da Associação de Integração Social de Itajubá - AISII

SUMÁRIO

ATUAÇÃO DO NOSSO COMITÊ

Por determinação da LGPD, foi criado o **Comitê Gestor de Proteção de Dados Pessoais – CGPD**, por intermédio de formação de equipe multidisciplinar do HCI.

O Comitê de Segurança da Informação pretende fiscalizar e deliberar sobre assuntos que estejam ligados direta ou indiretamente à questão dos dados pessoais no âmbito da Instituição. O referido comitê é gerenciado pelo encarregado ou *Data Protection Officer – DPO*, cujas atribuições envolvem cuidar das questões LGPD dentro do hospital, bem como atuar como canal de comunicação entre o titular de dados pessoais, a instituição e a Autoridade Nacional de Proteção de Dados – ANPD.

Foi elaborado o "Manual de Recomendações LGPD" que compõe parte do nosso processo de integração de colaboradores. Porém, a par do material já divulgado, verificamos também a necessidade da criação de uma Cartilha que abordasse o assunto de forma mais ampla e dinâmica, contendo diretrizes práticas que facilitassem o entendimento alusivo ao tratamento de dados na instituição. Nessa linha, construímos a presente Cartilha visando apoiar e incentivar a cultura de privacidade nos moldes da LGPD no HCI.

Para isso, seguiremos cinco pilares, quais sejam: preparação, organização, desenvolvimento, implementação de processos, governança e melhoria contínua. A presente cartilha poderá ser atualizada com base em novas regulamentações legais, para que nossa atuação evolua sempre, em busca da melhor prestação de serviço à sociedade.

Redação:
Mariana Rodrigues de Castro – Encarregada de Dados (DPO)
Revisão:
Seleno Glauber de Jesus Silva– Diretor Geral
Tiago José Magalhães – Diretor Jurídico
Formatação:
Ana Paula Gomes Vasconcelos – Assessora de Comunicação

GLOSSÁRIO

Para acompanhar esta cartilha, é importante compreender algumas definições:

Agentes De Tratamento: o controlador e o operador.

Anonimização: processos e técnicas por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Dados Pessoais: toda informação relacionada à pessoa natural identificada ou identificável, tal como nome, RG, CPF, e-mail etc.

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

Titular: pessoa natural a quem se referem os dados pessoais, que são objeto de tratamento.

DESMISTIFICANDO A LGPD PARA PROFISSIONAIS DE SAÚDE

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, sancionada em 14 de agosto de 2018, entrou em vigor em setembro de 2020 e marca um ponto crucial na proteção da privacidade de informações pessoais, tanto em formatos físicos quanto digitais.

A LGPD protege os indivíduos contra práticas prejudiciais comuns, como o envio de publicidade não solicitada, a venda inadequada de listas de contatos e fraudes realizadas por criminosos, entre outras situações similares.

Em 2022, a proteção de dados pessoais foi reconhecida como um direito fundamental na Constituição Federal, através de uma Emenda Constitucional, refletindo o avanço e a importância crescente da LGPD.

É importante lembrar que a LGPD não se aplica ao tratamento de dados pessoais para fins estritamente pessoais e não econômicos, bem como para atividades jornalísticas, artísticas, acadêmicas, de segurança pública, defesa nacional e investigações penais. De igual modo, também não é aplicável a dados relacionados a pessoas jurídicas, como razão social, CNPJ e endereço comercial.

OBJETIVOS DA LEI

Vivemos uma era de significativos avanços, especialmente no campo tecnológico e digital. Esses avanços impactam diretamente as informações pessoais dos indivíduos, pois os dados agora são valorizados e frequentemente comparados ao "novo petróleo".

A lei não proíbe nem restringe o tratamento de dados, algo que é essencial para a regulação do mercado. O principal objetivo é orientar e regulamentar a forma como esse tratamento deve ser realizado, garantindo assim direitos como a liberdade, a privacidade e a proteção contra discriminação.

Dessa forma, a lei oferece segurança jurídica para os responsáveis pelo tratamento de dados, ao mesmo tempo em que protege os direitos dos titulares das informações pessoais. Em termos amplos, a LGPD estabelece os seguintes objetivos:

- ✓ Introduzir no âmbito da Instituição o assunto de forma clara, simplificada e didática.
- ✓ Informar os conceitos, fundamentos e princípios da LGPD, a fim de nortear a atuação de todos que realizam qualquer tipo de tratamento de dados.
- ✓ Indicar agentes envolvidos e estruturar o ciclo de vida dos dados.
- ✓ Esclarecer os direitos dos titulares de dados pessoais.
- ✓ Fomentar a disseminação da cultura e governança em privacidade.

O SETOR DA SAÚDE JÁ POSSUI NORMAS DE PROTEÇÃO DE DADOS PESSOAIS?

- Resolução nº 1.821/2007 do CFM, que dispõe sobre o prontuário eletrônico de dados médicos, considerados sensíveis;
- Lei nº 12.965/2014, Marco Civil da Internet ("MCI"), que estabeleceu direitos, limites e obrigações de usuários e serviços de Internet, inclusive plataformas e aplicativos de saúde. A lei trata especificamente de questões ligadas ao uso de dados pessoais, tais como a necessidade de consentimento prévio, livre, específico e informado dos usuários, porventura pacientes;
- Resolução nº 1.605/2000 do CFM, que determina o compartilhamento de dados pessoais mediante consentimento do titular dos dados;
- Resolução nº 1643/2002 do CFM, que trata sobre a telemedicina e a necessidade de sigilo dos dados do paciente;
- Portaria nº 467/2020 do Ministério da Saúde, que trata sobre a utilização da telemedicina no período de controle da pandemia do coronavírus e trata sobre obrigação de sigilo dos dados do paciente;
- Resolução nº 466/2012 do Conselho Nacional de Saúde, que trata sobre a pesquisa clínica e do consentimento livre e esclarecido;
- Lei nº 13.787/18, que dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.

Logo, a LGPD não será o único dispositivo legal aplicado, devendo sempre haver interpretação harmônica e compatível com as demais normas legais e regulatórias aplicáveis ao setor.

AS NORMAS RESTRITIVAS DA LGPD SE APLICAM AOS EXERCÍCIOS DAS ATRIBUIÇÕES LEGAIS DO CONSELHO DE MEDICINA?

O Conselho Federal de Medicina (CFM) possui um histórico de estabelecer normas rigorosas para proteger o sigilo de dados pessoais, garantindo a confidencialidade profissional e a privacidade dos prontuários médicos. Essas diretrizes são fundamentais para o sigilo processual em casos ético-profissionais.

No entanto, é importante esclarecer que as normas restritivas da Lei Geral de Proteção de Dados Pessoais (LGPD) não impedem o Conselho de Medicina de acessar dados no exercício de suas atribuições legais.

O acesso a dados pessoais, incluindo informações sensíveis, realizado por médicos e demais profissionais no contexto de fiscalização pelo Conselho é permitido para o cumprimento de obrigações legais e regulamentares.

Portanto, a LGPD se aplica ao tratamento de dados pessoais em geral, mas não restringe a capacidade do CFM e de seus representantes de acessar essas informações quando necessário para o desempenho sua função regulamentar.

PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS

As atividades de tratamento de dados pessoais deverão observar principalmente a boa-fé e os seguintes princípios:

Finalidade: a realização do tratamento deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma diversa dessas finalidades;

Adequação: a compatibilidade do tratamento deve ocorrer conforme as finalidades informadas, de acordo com o contexto do tratamento;

Necessidade: o tratamento deve se limitar à realização de suas finalidades, coletando somente dados pertinentes, proporcionais e não excessivos em relação à sua finalidade.

Livre acesso: é a garantia de consulta livre, de forma facilitada e gratuita, à forma e à duração do tratamento, bem como à integralidade de seus dados pessoais;

Qualidade dos dados: é a garantia de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

Transparência: é a garantia de que haverá informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento;

Segurança: trata-se da utilização de medidas técnicas e administrativas qualificadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

Prevenção: compreende a adoção de medidas para prevenir a ocorrência de danos por causa do tratamento de dados pessoais;

Não discriminação: o tratamento dos dados não pode ser realizado para fins discriminatórios, ilícitos ou abusivos;

Responsabilização e prestação de contas: demonstração, pelo Controlador ou pelo Operador, de todas as medidas eficazes e capazes de comprovar o cumprimento da lei e a eficácia das medidas aplicadas.

AFINAL, O QUE É O TRATAMENTO DE DADOS PESSOAIS?

O tratamento de dados pessoais refere-se a qualquer operação realizada com informações que identificam ou podem identificar uma pessoa. Isso inclui atividades como coleta, armazenamento, uso, modificação, compartilhamento e exclusão desses dados.

Essas operações podem ser realizadas de diversas formas, incluindo manualmente (papéis e documentos físicos) ou por meio de sistemas digitais (bancos de dados, aplicativos e plataformas online).

O tratamento de dados pessoais é regido por leis e regulamentos específicos para garantir que esses dados sejam manejados de maneira segura e ética, respeitando a privacidade dos indivíduos.

QUAIS DADOS SÃO PROTEGIDOS PELA LGPD?

Dados Pessoais

São informações que identificam ou podem identificar uma pessoa natural, direta ou indiretamente. Exemplos incluem:

- Nome completo
- Endereço residencial
- Número de telefone
- Endereço de e-mail
- Número de documentos de identificação (como CPF e RG)
- Informações bancárias e financeiras

Dados Pessoais Sensíveis

São dados que, devido à sua natureza, podem implicar riscos significativos à privacidade dos indivíduos. A LGPD estabelece regras mais rigorosas para o tratamento desses dados. Exemplos:

- Dados sobre origem racial ou étnica
- Dados sobre convicções religiosas
- Dados sobre opiniões políticas
- Dados sobre saúde ou vida sexual
- Dados sobre a vida genética ou biométrica

Dados de Saúde

São informações relacionadas à saúde física ou mental do indivíduo, incluindo:

- Histórico médico
- Diagnósticos
- Tratamentos e medicamentos
- Exames e resultados laboratoriais
- Informações sobre condições de saúde

Dados Biométricos

São dados que podem identificar uma pessoa com base em características biológicas, fisiológicas ou comportamentais. Exemplos incluem:

- Impressões digitais
- Reconhecimento facial
- Íris dos olhos
- Voz

Importante:
A LGPD aplica-se ao tratamento de dados pessoais em geral, mas estabelece regras especiais para dados pessoais sensíveis devido ao seu potencial impacto à privacidade e à segurança dos indivíduos.

DIREITOS DOS TITULARES SOB A LGPD: GARANTIAS E PROTEÇÕES

A Lei Geral de Proteção de Dados, além de trazer obrigações para os controladores e operadores, traz direitos aos titulares dos dados, como:

- Confirmação da existência de tratamento.
- Acesso aos dados.
- Correção de dados.
- Anonimização, bloqueio ou eliminação de dados.
- Portabilidade dos dados.
- Eliminação dos dados tratados com consentimento.
- Informações sobre o compartilhamento de dados.
- Informação sobre a possibilidade de não fornecer consentimento.
- Revogação do consentimento.
- O direito do titular de dados de se manifestar contra o controlador na ANPD e nos órgãos de defesa do consumidor.
- O direito de opor-se ao tratamento realizado com dispensa de consentimento, caso não esteja em conformidade com a lei.

O titular dos dados tem o direito de solicitar informações sobre o tratamento de seus dados a qualquer momento. Para isso, poderá entrar em contato com o DPO pelo e-mail dpo@hcitajuba.org.br, preenchendo o formulário eletrônico disponível no site do HCI. O requerimento deve ser acompanhado da assinatura do titular dos dados ou de seu representante legalmente constituído. O exercício dos direitos dos titulares deve seguir os prazos e procedimentos estabelecidos na legislação aplicável, especialmente na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

A apresentação do requerimento é gratuita, exceto quando houver necessidade de reprodução de documentos, caso em que poderá ser cobrado apenas o valor necessário para ressarcir os custos com materiais. Entretanto, é importante destacar que nenhum direito é absoluto. Há situações em que a organização pode não atender ao requerimento do titular, devendo, nesse caso, informar os motivos, como o cumprimento de obrigações legais ou regulatórias.

COMUNICAÇÃO COM A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E COM OS TITULARES DE DADOS PESSOAIS (DPO)

O Encarregado pelo Tratamento de Dados Pessoais (DPO) é a pessoa designada para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). De acordo com a LGPD, as responsabilidades do DPO incluem:

- Receber e Gerenciar Reclamações: Aceitar reclamações e comunicações dos titulares de dados, fornecer esclarecimentos e tomar as medidas necessárias para resolver as questões apresentadas.
- Comunicação com a ANPD: Receber comunicações da ANPD e adotar as providências necessárias para atender às orientações e exigências da autoridade.
- Orientação Interna: Orientar funcionários e contratados sobre as práticas e procedimentos a serem seguidos para assegurar a proteção adequada dos dados pessoais.
- Execução de Atribuições: Realizar outras tarefas que sejam determinadas pelo controlador ou estabelecidas em normas complementares relacionadas à proteção de dados.

Essas funções garantem uma comunicação eficaz e o cumprimento das normas de proteção de dados, promovendo a transparência e a conformidade com a LGPD.

OBRIGAÇÕES E RESPONSABILIDADES

A Lei Geral de Proteção de Dados (LGPD), descreve várias obrigações e responsabilidades para garantir a proteção dos dados pessoais dos pacientes, colaboradores e demais interessados, aqui estão algumas das principais:

Consentimento: os hospitais devem obter o consentimento explícito dos pacientes para coletar e tratar seus dados pessoais, exceto em casos onde o tratamento seja necessário para cumprir obrigações legais ou regulatórias.

Finalidade Específica: os dados pessoais devem ser coletados para finalidades específicas, legítimas e informadas ao paciente, e não devem ser usados para outros fins sem novo consentimento.

Medidas de Segurança: implementar medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados, vazamentos, e outros tipos de violação.

Treinamento de colaboradores: garantir que os funcionários e colaboradores recebam treinamento adequado sobre práticas de proteção de dados e segurança da informação.

Informação ao Titular: fornecer informações claras sobre como os dados pessoais são coletados, utilizados, armazenados e compartilhados, incluindo o direito dos pacientes de acessar e corrigir seus dados.

Política de Privacidade: manter uma política de privacidade acessível que detalhe as práticas de tratamento de dados do hospital.

Compartilhamento: garantir que qualquer compartilhamento de dados pessoais com terceiros (como prestadores de serviços ou outras instituições) seja feito com base em contratos e documentos que garantam a conformidade com a LGPD.

Atendimento a Solicitações: facilitar e atender as solicitações dos titulares de dados para acessar, corrigir, excluir ou portar seus dados pessoais.

Notificação de Incidentes: notificar imediatamente o Encarregado de Dados (DPO) e, se for o caso, a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares em caso de incidentes que possam acarretar risco ou dano.

Designação de Encarregado: nomear um encarregado pelo tratamento de dados pessoais (DPO - Data Protection Officer) que será responsável por garantir a conformidade com a LGPD e atuar como ponto de contato para questões relacionadas à proteção de dados.

Registros: manter registros detalhados das atividades de tratamento de dados, incluindo finalidades, tipos de dados tratados, bases legais, e medidas de segurança adotadas.

Relatórios de Conformidade: elaborar e revisar relatórios sobre a conformidade com a LGPD e fornecer informações à ANPD quando necessário.

FISCALIZAÇÕES E SANÇÕES

A LGPD elenca as sanções administrativas para o caso de descumprimento de seus preceitos:

- Advertência com indicação de prazo para adoção de medidas corretivas;
- Multa simples de até 2% limitada a R$ 50 milhões do faturamento da pessoa jurídica de direito privado por infração;
- Multa diária;
- Publicização da infração;
- Bloqueio dos dados pessoais a que se refere a infração até sua regularização;
- Eliminação dos dados pessoais a que se refere a infração;
- Suspensão do tratamento dos dados pessoais a que se refere a infração;
- Proibição parcial ou total de exercer atividades de tratamento de dados.

Lembrando que todas essas sanções são administrativas. Ou seja, é possível ainda que haja eventual responsabilização por danos na esfera judicial!

ATENÇÃO AO PROTOCOLO DE ATENDIMENTO HOSPITALAR

O Protocolo de Atendimento descreve os principais momentos em que os dados dos pacientes são coletados e processados, bem como os tipos de dados envolvidos. Esses momentos incluem:

Entrada do Paciente: fornecimento de dados cadastrais na admissão.
Consulta Médica: manipulação e atualização do prontuário do paciente.
Exames Laboratoriais: coleta e análise dos dados relacionados aos exames.

Em situações emergenciais ou não, os hospitais utilizam dados pessoais dos pacientes para:
Identificação: confirmar a identidade do paciente.
Avaliação da Saúde: realizar anamnese para verificar parâmetros vitais.

Esses dados são registrados no prontuário médico, um documento essencial para o histórico de saúde do paciente, tanto em hospitais quanto em clínicas.

Dados de Visitantes e Acompanhantes

Os hospitais também lidam com dados pessoais de visitantes e acompanhantes. Estes dados devem ser tratados com o mesmo cuidado e conforme as regras estabelecidas pela Lei Geral de Proteção de Dados Pessoais (LGPD).

PRINCIPAIS BASES LEGAIS

As bases legais da LGPD são como regras que explicam quando e por que você pode coletar, usar e compartilhar dados pessoais de alguém. Para um hospital, essas bases são importantes para garantir que o tratamento das informações dos pacientes de forma correta e legal. Aqui estão as principais bases legais que um hospital deve conhecer:

Execução de Contrato

Será legítima a utilização sempre que houver a necessidade da manipulação de informações pessoais, advinda de uma obrigação contratual em que o titular de dados seja parte, para atingir a finalidade da prestação do serviço solicitado. Abrange contratos de prestação de serviços de saúde, como a contratação de consultas e exames.

Consentimento

O consentimento não é a única hipótese legal para que um controlador trate dados pessoais. A LGPD elenca todas as possibilidades para que o tratamento de dados pessoais seja realizado de forma regular. O consentimento é apenas uma dessas hipóteses e não possui nenhuma prioridade sobre as outras.

Ao controlador dos dados compete a decisão de qual a melhor hipótese legal para o tratamento dos dados que ele realiza. O consentimento, quando aplicável, deverá referir-se a finalidades determinadas e ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

O consentimento pode ser revogado a qualquer momento mediante manifestação expressa, por procedimento gratuito e facilitado.

É importante esclarecer que o Termo de Consentimento Livre e Esclarecido (TCLE) e o consentimento previsto pela Lei Geral de Proteção de Dados (LGPD) são instrumentos distintos, com origens e objetivos diferentes. Embora ambos envolvam o conceito de consentimento, eles são aplicados de maneiras específicas:

Termo de Consentimento Livre e Esclarecido (TCLE): é um documento que garante que o indivíduo foi informado de maneira completa e compreendeu todos os aspectos do atendimento, incluindo riscos e benefícios. Ele é um requisito ético e regulamentar para garantir a transparência e o respeito pelo titular.

Consentimento na LGPD: a LGPD exige que o consentimento seja uma das bases legais para o tratamento de dados pessoais e sensíveis, incluindo dados de saúde. O consentimento sob a LGPD deve ser livre, informado e explícito, e deve permitir ao titular dos dados conhecer a finalidade do tratamento, a natureza dos dados coletados e a possibilidade de revogação a qualquer momento.

Atenção! Consentimento Especial para Crianças e Adolescentes

O tratamento de dados pessoais de crianças e adolescentes exige uma atenção especial. O consentimento para o tratamento desses dados deve ser obtido de maneira específica e destacada.

Este tratamento só pode ser realizado mediante o consentimento explícito de pelo menos um dos pais ou do responsável legal.

Essa exigência pode trazer dificuldades práticas, já que, em alguns casos, estabelecimentos que lidam com dados pessoais de crianças, sobretudo em se tratando de hospitais, estão atuando com situações emergenciais, nas quais não haverá tempo hábil para a coleta prévia do consentimento dos pais.

Para ocasiões como essa, a lei traz uma exceção, que permite eventual tratamento de dados pessoais de crianças sem o consentimento exigido. O objetivo é garantir a proteção da vida da criança. Nesse caso, os dados podem ser utilizados uma única vez e sem armazenamento. Mas, sob hipótese alguma, podem ser repassados a terceiros.

É essencial implementar medidas adicionais de proteção e segurança para garantir que os dados de crianças e adolescentes sejam tratados com o máximo cuidado e conforme as diretrizes da LGPD.

Obrigação Regulatória: Notificações Compulsórias

De acordo com a Lei Geral de Proteção de Dados (LGPD), algumas obrigações regulatórias exigem que as instituições de saúde realizem notificações compulsórias, mesmo no contexto da proteção de dados pessoais.

Um exemplo importante é a notificação à Secretaria de Saúde do Município sobre resultados de exames para doenças, agravos ou eventos.

Em conformidade com as regulamentações de saúde pública, os hospitais e instituições de saúde têm a obrigação de notificar as autoridades de saúde competentes sobre determinados resultados de exames que indicam doenças, agravos ou eventos de notificação compulsória.

Embora a notificação deva ocorrer para cumprir com obrigações legais, a instituição ainda deve garantir que a transmissão das informações seja feita de maneira segura. É dever que apenas os dados necessários para o cumprimento da obrigação legal sejam compartilhados, evitando a divulgação de informações excessivas.

É importante que a Instituição informe os pacientes sobre as situações em que seus dados podem ser compartilhados com autoridades de saúde.

A Instituição deve manter registros apropriados das notificações realizadas, incluindo as bases legais e os procedimentos seguidos, para garantir a conformidade com a LGPD e facilitar auditorias e verificações.

Tutela da saúde

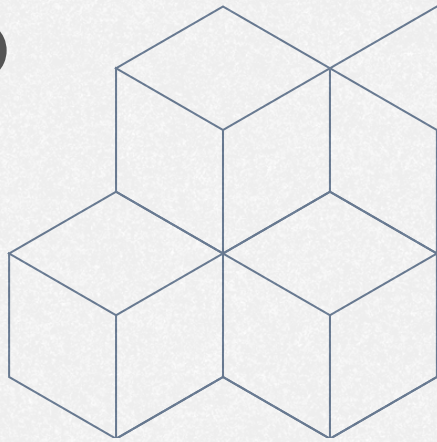
A tutela da saúde refere-se ao tratamento de dados pessoais, especialmente dados sensíveis relacionados à saúde, para fins de proteção e cuidado com a saúde pública e individual. Esse tratamento deve atender a várias exigências para garantir que os direitos dos titulares dos dados sejam respeitados.

A tutela da saúde permite que instituições de saúde, profissionais médicos e entidades sanitárias tratem dados sensíveis relacionados à saúde sem necessidade de consentimento adicional, desde que o tratamento esteja alinhado com as finalidades específicas e regulamentações aplicáveis.

Embora o tratamento para a tutela da saúde não exija consentimento explícito em muitos casos, é fundamental que os titulares sejam informados sobre o tratamento de seus dados e tenham acesso às informações necessárias para compreender como seus dados são usados.

Além da LGPD, o tratamento de dados para tutela da saúde pode estar sujeito a outras regulamentações específicas do setor de saúde, como normas de entidades reguladoras e leis locais que regulam a proteção e gestão de dados de saúde.

GESTÃO E PROTEÇÃO DO PRONTUÁRIO MÉDICO



De acordo com o artigo 1º da Resolução 1.638/2002 do Conselho Federal de Medicina (CFM), o prontuário médico é definido como um "documento único constituído de um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada."

A elaboração e a guarda do prontuário médico são responsabilidades do profissional de saúde que presta a assistência e do estabelecimento de saúde. Existem normas legais que regulam o acesso a esses documentos.

O prontuário médico é um documento sigiloso e não pode ser compartilhado sem o consentimento esclarecido do paciente. A produção de fotos, fotocópias, digitalizações ou cópias digitais do prontuário, total ou parcial, só é permitida com autorização prévia e por escrito do paciente, salvo outras situações previstas legalmente.

É proibido retirar, adulterar ou destruir qualquer documento do prontuário, bem como fazer comentários verbais ou eletrônicos sobre os dados do paciente sem autorização.

O acesso ou a liberação do prontuário, ou de partes dele, fora das regras estabelecidas é considerado ilegal e pode ter consequências tanto para o profissional quanto para a instituição.

Os profissionais de saúde devem garantir a segurança do prontuário e possibilitar o acesso ao paciente quando solicitado. A recusa em fornecer o prontuário, quando requisitado, não só viola a LGPD, mas também constitui uma infração ética.

A norma exige que sejam implementadas medidas rigorosas para prevenir o acesso não autorizado. A utilização de senhas individuais e o estabelecimento de restrições de acesso baseadas no cargo do profissional são práticas recomendadas.

APLICABILIDADE NA ASSISTÊNCIA DE ENFERMAGEM

A equipe de enfermagem desempenha um papel crucial em diversos contextos de saúde, desde a atenção primária em ambulatórios até a internação hospitalar. Em todos esses ambientes, a enfermagem gerencia dados sensíveis através dos registros de saúde dos pacientes. Para garantir a proteção desses dados, é fundamental que os profissionais de enfermagem estejam atualizados e cientes das normas relacionadas à privacidade e à segurança dos dados, conforme a Lei Geral de Proteção de Dados (LGPD).

Registro e Acesso ao Prontuário: nos prontuários eletrônicos, o acesso é restrito aos profissionais contratados pela instituição, o que está alinhado com a LGPD. No entanto, a lei incentiva uma abordagem ainda mais restritiva, permitindo o acesso e registro de dados apenas por profissionais diretamente envolvidos no cuidado do paciente. Isso não só protege o paciente, mas também a instituição e os profissionais de enfermagem.

Conformidade com o COFEN: as diretrizes da LGPD são coerentes com as exigências do Conselho Federal de Enfermagem (COFEN). Os princípios da LGPD alinham-se aos já estabelecidos pelo Código de Ética dos Profissionais de Enfermagem, reforçando a importância do sigilo e da proteção dos dados do paciente.

Prevenção de Acesso Não Autorizado: a equipe de enfermagem deve adotar práticas preventivas para evitar acessos não autorizados e o mau uso dos dados. É essencial evitar vazamentos e garantir que os dados sejam utilizados exclusivamente para fins relacionados à saúde.

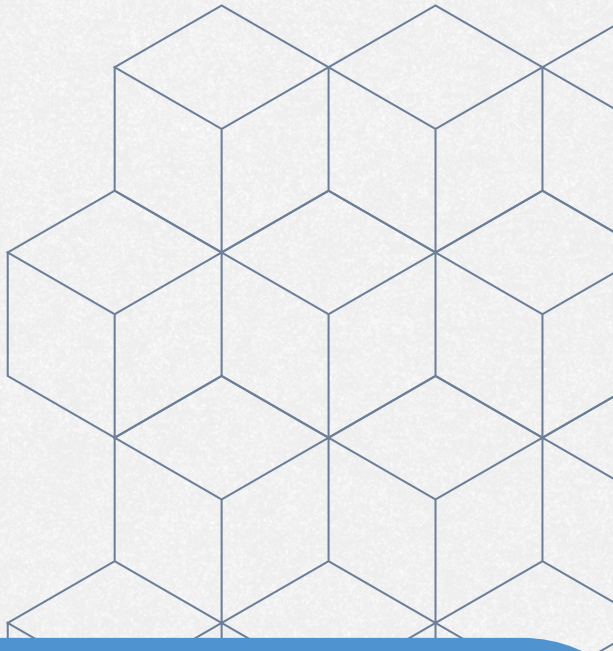
Responsabilidades Legais e Administrativas: o não cumprimento da LGPD pode resultar em responsabilizações civis perante a instituição de saúde ou o paciente, além de processos judiciais. Também pode haver penalidades administrativas impostas pela Autoridade Nacional de Proteção de Dados (ANPD).

Consequências Ético-Disciplinar: a violação das normas de sigilo e proteção de dados pode levar a sanções ético-disciplinares, refletindo o descumprimento do dever de sigilo estabelecido pelo Código de Ética dos Profissionais de Enfermagem.

A conformidade com a LGPD é essencial para a proteção dos dados pessoais dos pacientes e para a manutenção da confiança entre a equipe de enfermagem, corpo clínico e os pacientes. A adesão às práticas recomendadas e o cumprimento das normas são fundamentais para garantir a segurança e a privacidade das informações de saúde.

RESOLUÇÃO DE INCIDENTES DE SEGURANÇA: PREVENÇÃO, RESPOSTA E MELHORIA CONTÍNUA

O programa de proteção de dados pessoais do HCI estabelece uma política para lidar com incidentes de segurança da informação, que inclui a comunicação imediata ao Encarregado de Dados (DPO), Autoridade Nacional (ANPD) e ao titular dos dados pessoais. Incidentes de segurança referem-se a violações das normas da LGPD, especialmente no que diz respeito à privacidade e ao sigilo dos dados mantidos pelo hospital, enquanto controlador.

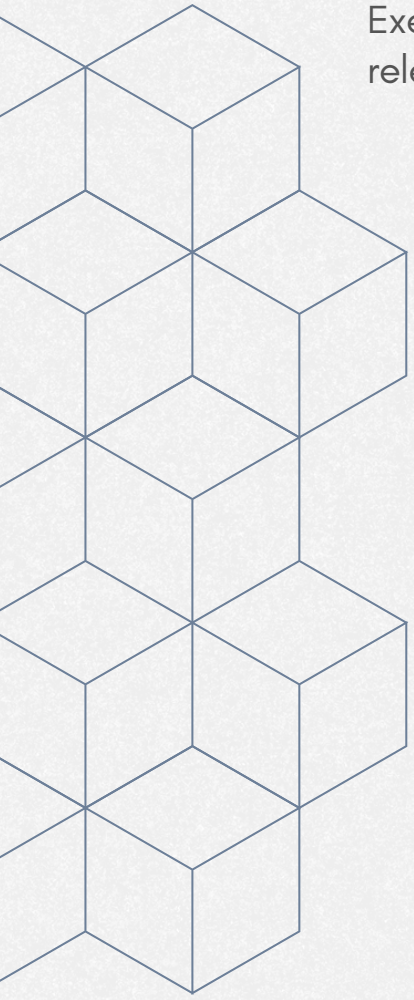


A gestão de incidentes de segurança envolve como principais pilares:

- **Detecção:** Monitoramento de sistemas e redes para identificar possíveis incidentes de segurança.
- **Resposta:** Implementação de um plano de resposta a incidentes que inclua análise de impacto, contenção, erradicação e recuperação.
- **Notificação:** Informar a ANPD e os titulares dos dados conforme os requisitos da LGPD, se o incidente representar risco ou dano relevante.
- **Revisão:** Após a resolução do incidente, é necessário revisar os procedimentos e atualizar as políticas para prevenir ocorrências futuras.

De acordo com a LGPD, o controlador deve informar à autoridade nacional e ao titular sobre qualquer incidente de segurança que possa causar risco ou dano significativo aos titulares no prazo de três (3) dias úteis.

Portanto, nem todos os incidentes de segurança necessitam de comunicação à ANPD. O controlador deve avaliar os riscos e impactos para os titulares resultantes do incidente e determinar se a comunicação é realmente necessária.



Exemplos de incidentes que podem causar risco ou dano relevante aos titulares incluem:

- A indisponibilidade prolongada de um sistema em uma rede hospitalar devido a um sequestro de dados, que pode impedir o acesso às informações dos pacientes e comprometer procedimentos médicos, expondo dados pessoais sensíveis e colocando a saúde dos titulares em risco.

- A perda ou roubo de documentos ou dispositivos que contenham dados pessoais protegidos por sigilo profissional, cópias de documentos de identificação oficial e dados de contato dos titulares, o que pode resultar em riscos reputacionais e possíveis fraudes financeiras.

Qualquer tratamento inadequado ou violação dos dados pessoais pode acarretar responsabilidades. Por isso, é crucial manter comunicação constante com o Encarregado de Proteção de Dados (DPO) para assegurar o monitoramento e a implementação de ações corretivas, além de interagir com os órgãos de investigação e a ANPD para minimizar rapidamente os impactos aos titulares dos dados.

A comunicação voluntária do incidente pelo controlador demonstra transparência, cooperação e boa-fé, e será considerada em eventuais processos de fiscalização ou ações administrativas e judiciais.

CONFORMIDADE E QUALIDADE: A RELAÇÃO ENTRE A LGPD E A GESTÃO HOSPITALAR EFICIENTE

A relação entre a Lei Geral de Proteção de Dados Pessoais (LGPD) e a gestão da qualidade em um hospital é crucial para garantir que a instituição não apenas ofereça cuidados médicos de alta qualidade, mas também proteja as informações pessoais e sensíveis de seus pacientes de acordo com a legislação.

O setor de qualidade, deve garantir que os processos de proteção de dados sejam robustos e eficazes. Isso inclui a implementação de medidas de segurança, como criptografia, controle de acesso e treinamento de pessoal para garantir que dados sensíveis, como históricos médicos e informações pessoais, sejam manejados com a máxima segurança.

Deve-se ainda garantir processos e protocolos para a coleta, armazenamento e uso de dados pessoais estejam claramente definidos e praticados. Isso ajuda a garantir que o hospital não apenas atenda aos requisitos de qualidade em termos de cuidados médicos, mas também esteja em conformidade com as exigências da LGPD.

Esse trabalho exige uma análise de riscos detalhada. Em um hospital, isso pode envolver a identificação de riscos relacionados à proteção de dados, como vulnerabilidades em sistemas de TI ou práticas inadequadas de manuseio de informações, e o desenvolvimento de estratégias para mitigá-los.

Para o HCI, integrar a LGPD com a gestão da qualidade é fundamental para garantir que a proteção de dados pessoais e a prestação de cuidados médicos estejam alinhadas. Além de proteger a privacidade dos pacientes e a cumprir a legislação, também contribui para a qualidade geral dos serviços prestados e para a confiança dos pacientes na instituição. A gestão eficaz de dados e a qualidade dos cuidados são interdependentes e devem ser abordadas de forma integrada para alcançar os melhores resultados possíveis.

PAPEL DA LGPD NA SEGURANÇA DA INFORMAÇÃO HOSPITALAR: O QUE VOCÊ PRECISA SABER

A segurança da informação é essencial para a proteção dos dados pessoais dos pacientes e para a conformidade com a LGPD. Implementar medidas eficazes de segurança, manter processos e procedimentos claros, e garantir a formação contínua dos funcionários são passos cruciais para um ambiente hospitalar seguro e em conformidade com a legislação.

Para tanto, é crucial reforçar as medidas de segurança por meio de auditorias periódicas. As seguintes práticas devem ser implementadas:

Controle e Restrições de Acesso: estabeleça medidas rigorosas de controle de acesso para assegurar que apenas pessoas autorizadas possam acessar documentos e informações sensíveis.

Monitoramento de Dados: adote sistemas que rastreiem todas as atividades realizadas com os dados, incluindo modificações, cópias e compartilhamentos, para garantir a integridade e a segurança das informações.

Validação de Transferências de Arquivos: implemente um sistema para validar as transferências de arquivos, garantindo que os dados sejam movidos de forma segura e autorizada.

Também é necessário cuidado em relação à possibilidade de roubo de identidade médica, que pode ocorrer por meio da usurpação ou identificação das credenciais de um usuário em um sistema, devendo o sistema de autenticação ser reforçado (como a utilização do método de dois fatores de identificação).

Estas práticas, se aplicadas de forma correta, ajudam a proteger os dados pessoais e a assegurar um ambiente de segurança robusto e eficaz.

BOAS PRÁTICAS PARA SEGURANÇA E PRIVACIDADE DE DADOS

O não cumprimento das medidas preventivas pode resultar em sanções mais severas em um eventual processo administrativo. Portanto, é crucial adotar posturas de colaboração e prevenção para garantir a conformidade com as normas de segurança e privacidade de dados. A seguir, estão algumas boas práticas essenciais para proteger dados pessoais e manter a segurança da informação.

O que Fazer para Contribuir para a Adequação:

- **Trocar Periodicamente as Senhas:** realize a troca de senhas regularmente para garantir a segurança das contas.
- **Descartar Documentos de Forma Correta:** use um fragmentador de papel para eliminar documentos que contenham dados pessoais.
- **Utilizar a Função de Bloqueio:** sempre bloqueie seu computador ao se ausentar da estação de trabalho.
- **Reportar Falhas de Segurança:** informe imediatamente ao DPO sobre qualquer falha de segurança ou violação da LGPD.

- **Seguir Normas e Políticas:** observe as normas aplicáveis, políticas e boas práticas adotadas pelo HCI ao tratar dados pessoais.
- **Reduzir Riscos:** minimize os riscos relacionados à segurança da informação em todas as suas atividades.
- **Evitar Acesso Não Autorizado:** proteja o banco de dados do HCI contra acessos não autorizados.
- **Limitar Acesso a Dados:** proteja o banco de dados do HCI contra acessos não autorizados.
- **Tratar Dados Dentro das Atribuições :** realize o tratamento de dados pessoais conforme suas responsabilidades.
- **Eliminar Dados Desnecessários:** descarte dados pessoais que não têm mais justificativa para manutenção, seguindo as orientações da chefia e do(a) Encarregado(a) pelo tratamento de dados, bem como as normas internas

O que Evitar para Contribuir para a Adequação:

- **Não Deixar Documentos à Vista:** evite deixar papéis ou documentos com dados pessoais expostos na impressora, copiadora ou na sua mesa.
- **Não Fotografar ou Filmar Documentos:** não tire fotos nem filme documentos que contenham dados pessoais.
- **Não Deixar a Tela Aberta:** não deixe a tela do computador visível quando estiver ausente da estação de trabalho.
- **Evitar Coletar Informações Desnecessárias:** não colete dados pessoais além do necessário para a finalidade específica.
- **Não Abrir E-mails Suspeitos:** evite abrir e-mails de origem duvidosa.
- **Não Utilizar Dados Desatualizados:** não use dados pessoais desatualizados ou incorretos.
- **Não Enviar E-mails Excessivos:** evite enviar e-mails para pessoas ou grupos maiores do que o necessário.
- **Não Fornecer Dados por Canais Inadequados:** não forneça dados pessoais por e-mail de origem suspeita, telefone ou outros canais não seguros.

POLÍTICA DE PRIVACIDADE PARA NAVEGAÇÃO NO SITE DO HCI

O HCI está comprometido com a proteção da sua privacidade e com a conformidade com a LGPD. Para garantir a segurança e a confidencialidade dos dados dos nossos usuários, adotamos uma série de medidas e práticas que fazem parte do nosso programa de governança da privacidade.

Isso inclui o aprimoramento contínuo das ferramentas tecnológicas, a implementação de medidas de segurança técnica e administrativa, bem como o fortalecimento dos controles, processos internos e da nossa organização.

Para entender como coletamos, utilizamos e protegemos suas informações pessoais e para acessar detalhes sobre nossos procedimentos de privacidade, visite nossa política de privacidade: hcitajuba.org.br

Se tiver qualquer dúvida ou precisar de mais informações, não hesite em nos contatar. Estamos à disposição para garantir que sua experiência conosco seja segura e em conformidade com as normas de privacidade.

CANAIS DE CONTATO

Encarregado de Dados – DPO: Mariana Rodrigues de Castro

E-mail: dpo@hcitajuba.org.br