

Curso de LGPD para Hospitais

Material Completo em PDF

Proteção de Dados Sensíveis em Ambiente Clínico

Introdução

A Lei Geral de Proteção de Dados (LGPD) estabelece normas para o tratamento de dados pessoais no Brasil. Em um hospital, onde circulam informações extremamente sensíveis sobre pacientes, colaboradores e terceiros, a LGPD exige cuidados redobrados e protocolos rígidos.

Este material foi criado para orientar profissionais da saúde e áreas administrativas sobre como aplicar a LGPD no ambiente hospitalar, garantindo segurança, confidencialidade e conformidade legal.

Módulo 1 – Fundamentos da LGPD no Hospital

1.1 O que é a LGPD e por que ela importa

A LGPD (Lei 13.709/2018) regula qualquer tratamento de dados pessoais realizado por empresas, profissionais e instituições públicas ou privadas.

Nos hospitais, ela é ainda mais crítica porque:

- o volume de dados é enorme;
- os dados são extremamente sensíveis;
- erros podem gerar danos irreparáveis aos pacientes;
- o hospital pode sofrer multas, punições e danos à reputação.

1.2 Conceitos fundamentais

Dado pessoal

Informação relacionada a uma pessoa identificada ou identificável.

Exemplos:

- Nome
- Telefone
- Endereço
- E-mail
- RG e CPF

Dado sensível (o mais importante para o hospital)

Informações que, se expostas, podem causar discriminação.

Exemplos:

- Informações de saúde

- Diagnósticos
- Exames
- Histórico médico
- Dados biométricos
- Raça, religião, orientação sexual

Titular dos dados

Qualquer pessoa física a quem os dados pertencem: pacientes, acompanhantes, visitantes, médicos, colaboradores.

Controlador

O hospital — decide como e por que os dados são utilizados.

Operador

Profissionais e sistemas que tratam os dados conforme orientação do hospital.

Encarregado (DPO)

Responsável por monitorar, orientar e comunicar questões de privacidade.

Módulo 2 – Dados Sensíveis no Hospital

2.1 Exemplos de dados sensíveis hospitalares

- Prontuário físico ou eletrônico
- Exames de imagem (raio-x, tomografia, ressonância)
- Laudos laboratoriais
- Dados de internação
- Diagnósticos e evolução do paciente
- Informações de gestantes, menores ou idosos
- Dados biométricos de colaboradores

2.2 Ciclo de vida dos dados no hospital

Coleta

Formulários, recepção, exames, sistemas de registro.

Armazenamento

Servidores internos, sistemas de prontuário, arquivos físicos.

Uso

Equipe médica, enfermeiros, administrativo, laboratórios.

Compartilhamento

Convênios, familiares autorizados, outros hospitais.

Descarte

Destruição segura conforme norma da ANS e do Ministério da Saúde.

Módulo 3 – Condutas Obrigatórias no Hospital

3.1 Acesso à informação

- A regra é: **acesso somente ao necessário para o trabalho**
- NUNCA utilizar login de outra pessoa
- NUNCA deixar tela destravada
- Evitar conversas sobre pacientes em corredores ou elevadores

3.2 Condutas proibidas

- Imprimir prontuários sem necessidade
- Fotografar documentos ou telas do sistema
- Usar WhatsApp pessoal para enviar dados de pacientes
- Compartilhar informações com terceiros sem autorização formal
- Deixar papéis com dados pessoais à vista

3.3 Boas práticas

- Trancar telas ao se afastar
 - Descartar documentos em caixas de destruição
 - Conferir a impressão e evitar deixar papéis na bandeja
 - Usar o sistema oficial do hospital para todo registro
-

Módulo 4 – Segurança da Informação na Saúde

4.1 Senhas e autenticação

- Senhas fortes (mínimo 8 dígitos, letras, números e símbolos)
- Trocar senhas periodicamente
- Não compartilhar usuário ou senha
- Ativar verificação em dois fatores, quando disponível

4.2 Dispositivos e redes

- Usar apenas computadores e celulares autorizados
- Evitar redes Wi-Fi abertas
- Pendrives são proibidos em setores críticos
- Sistemas devem ser acessados somente através de conexões seguras

4.3 Como identificar incidentes

- Computador lento ou com janelas estranhas
- Arquivos desaparecendo
- E-mails suspeitos pedindo “urgência”
- Sistemas fora do ar sem motivo claro

Se notar qualquer sinal, comunicar imediatamente ao setor responsável.

Módulo 5 – Incidentes, Penalidades e Responsabilidades

5.1 Penalidades

- Multas de até 2% do faturamento
- Responsabilidade civil do profissional
- Advertências e desligamento
- Processos judiciais
- Danos irreversíveis à reputação do hospital

5.2 O que fazer em caso de incidente

1. Não apagar nada
2. Informar imediatamente o setor de TI ou o DPO
3. Relatar o ocorrido com clareza
4. Seguir orientações da equipe de segurança
5. Registrar o incidente no sistema interno

O prazo para comunicação formal é rápido – até 72 horas em alguns casos.

Módulo 6 – Avaliação Final

A prova contém 10 perguntas de múltipla escolha.

Nota mínima: 70%.

O aluno tem até 3 tentativas.

Exemplos de questões

1. O que caracteriza um dado sensível?
2. É permitido enviar dados de pacientes pelo WhatsApp pessoal?
3. O que é o princípio do "need to know"?
4. Qual é o primeiro passo ao identificar um incidente?
5. O que deve ser feito com impressões esquecidas na bandeja?

Materiais Complementares

- Cartilha: Boas práticas de privacidade no hospital
- Modelo: Formulário de Comunicação de Incidentes
- Infográfico: Ciclo de vida dos dados hospitalares
- Checklist: Condutas obrigatórias de profissionais da saúde

Conclusão

A proteção de dados no ambiente hospitalar é uma responsabilidade de todos.

A aplicação correta da LGPD garante:

- mais segurança
- mais confiança dos pacientes
- menos riscos legais
- um ambiente profissional responsável

A privacidade é parte essencial do cuidado em saúde.

...