CARTILHA DE PROTEÇÃO DE DADOS PESSOAIS DA SPCC

Um guia rápido para quem cuida da vida e da informação

HCP 80 anos
TRATANDO A VIDA COM AMOR

HCP GESTÃO

POR QUE ESTA CARTILHA É IMPORTANTE?

Cuidar da saúde de alguém vai além do atendimento clínico. Significa também proteger a privacidade e os dados de quem confiou no Hospital de Câncer de Pernambuco (HCP) ou em alguma das unidades do HCP Gestão. Todos que trabalham, do atendimento à assistência, têm papel direto na segurança das informações dos nossos pacientes, acompanhantes, colegas e demais colaboradores.

Esta cartilha orienta você a saber o que fazer (e o que não fazer) em situações do dia a dia que envolvem o uso, o acesso, o descarte ou o compartilhamento de dados pessoais, conforme a Lei Geral de Proteção de Dados Pessoais (LGPD).

QUEM DEVE LER ESTA CARTILHA?

Colaboradores do Hospital de Câncer de Pernambuco e HCP Gestão.

O QUE SÃO DADOS PESSOAIS?

Dados pessoais são informações que identificam uma pessoa, seja de forma direta ou indireta, como:

- Nome completo
- CPF, RG, cartão do SUS
- Telefone
- Endereço
- Resultado de exames
- Imagens de câmeras de segurança
- Dados bancários
- Raça, cor, descrição, filiações partidárias
- Placa do carro ou habilitação

A EQUIPE DE PRIVACIDADE E O DPO

No HCP e HCP Gestão, a equipe de Privacidade é responsável por orientar que os dados pessoais de pacientes, acompanhantes, colaboradores e parceiros sejam tratados com segurança, seguindo a LGPD. Pense neles como os "guardiões" dos dados pessoais. Essa equipe conduz, monitora e atua em situações que envolvam o uso das informações, desde o cadastro até o descarte.

Já o **DPO (Data Protection Officer)**, ou encarregado de dados, é o profissional que representa o HCP e HCP Gestão na proteção dessas informações e desempenha um papel importante na comunicação entre os titulares, a organização e a ANPD -Autoridade Nacional de Proteção de Dados.

QUANDO DEVO FALAR COM A EQUIPE DE PRIVACIDADE OU DPO?

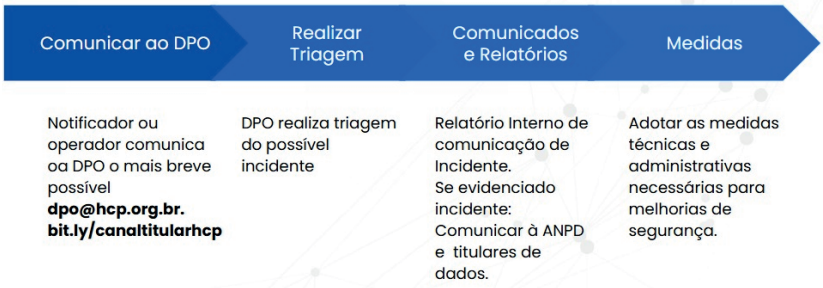
1. **Suspeita ou confirmação de vazamento de dados:** Se você notar qualquer atividade incomum em sistemas, acesso não autorizado a informações, perda de documentos ou dispositivos contendo dados pessoais (de pacientes, colaboradores ou terceiros), ou qualquer outra situação que possa ter comprometido a segurança dos dados.

2. **Desenvolvimento ou modificação de novos processos, sistemas ou tecnologias que envolvam dados pessoais:**
Antes de implementar uma nova ferramenta de gestão de pacientes, um aplicativo de telemedicina, um sistema de inteligência artificial para análise de exames, ou mesmo ao alterar significativamente a forma como os dados são coletados, usados, compartilhados, eliminados ou armazenados.

RESUMINDO:

Qualquer situação que possa colocar em risco a privacidade ou a segurança dos dados pessoais deve ser comunicada à Equipe de Privacidade ou ao DPO. Na dúvida, pergunte!

FLUXO DA COMUNICAÇÃO



Como entrar em contato com a equipe de Privacidade:

E-mail: dpo@hcp.org.br

O QUE NÃO FAZER COM DADOS PESSOAIS:

- Não compartilhar dados (imagens, nome, telefone, etc) de pacientes por telefone, WhatsApp ou e-mail.
- Salvar informações sigilosas em pendrives ou computadores pessoais.
- Acessar prontuários de pacientes que você não está atendendo.
- Discutir casos clínicos em ambientes públicos (refeitório, ônibus, elevador).

BOAS PRÁTICAS AO LIDAR COM INFORMAÇÕES PESSOAIS:

- Use senhas seguras e nunca as compartilhe.
- Bloqueie o computador ao se ausentar.
- Descaracterize os documentos antes de descartá-los.
- Oriente pacientes e acompanhantes com cuidado e respeito quanto ao uso dos dados pessoais.
- Reporte ao DPO qualquer situação incomum.
- Não utilizar os dados para finalidades diferentes para os quais foram coletados ou consentidos.

SOLICITAÇÕES E DIREITOS DOS TITULARES DE DADOS:

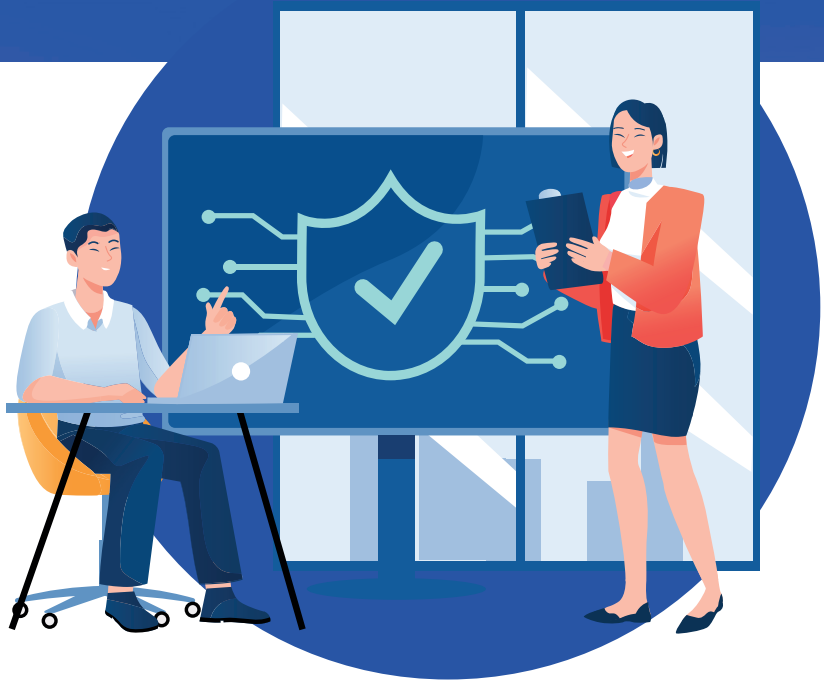
Se um paciente ou colaborador fizer uma solicitação relacionada aos seus direitos sobre seus dados pessoais, o colaborador que receber essa solicitação deve saber que:

Esses direitos são garantidos pela Lei Geral de Proteção de Dados (LGPD).

As solicitações podem envolver coisas como:

- Saber como as unidades de saúde estão tratando os dados pessoais.
- Ter acesso aos dados pessoais.
- Pedir correções, exclusões, bloqueios ou anonimização.
- Saber com quem os dados foram compartilhados.
- Pedir portabilidade dos dados.
- Revogar consentimentos previamente concedidos.

Em todos esses casos, oriente a realizar a solicitação no Canal de Comunicação do portal da privacidade www.hcp.org.br/privacidade-e-seguranca/ ou acione imediatamente a equipe de Privacidade.



SOBRE NOVOS PROCESSOS E TECNOLOGIAS:

Antes de implementar qualquer novo sistema ou tecnologia que envolva o tratamento de dados pessoais, é necessário garantir a proteção da privacidade e a aplicação de todas as medidas de segurança em conformidade com a LGPD.

Na dúvida, entre em contato com o DPO.

EXEMPLOS DE COMO A SEGURANÇA DE DADOS PESSOAIS PODE ESTAR AMEAÇADA E VOCÊ NÃO SABIA.

- Você percebe que um colega que está de férias teve sua senha usada para acessar dados de pacientes.
- O setor de marketing quer enviar e-mails para os pacientes sobre novos serviços do hospital e não possui o consentimento deles.
- O hospital vai fazer uma parceria com um laboratório, clínicas ou outras instituições e precisará compartilhar dados de pacientes.

- Tirar foto do prontuário ou do exame de um paciente com o celular, mesmo que para “ajudar” um colega ou pedir uma segunda opinião.

- Deixar um prontuário ou resultados de exames aberto em cima da mesa, na copa ou em qualquer área de circulação.

- Sair da estação de trabalho sem bloquear a tela do computador é como deixar a porta aberta. Acessos indevidos podem acontecer, permitindo a visualização e até a alteração de dados no sistema.

- Jogar exames, laudos ou fichas de pacientes diretamente na lixeira comum é uma ameaça séria. Esses documentos podem ser facilmente resgatados por pessoas mal-intencionadas.

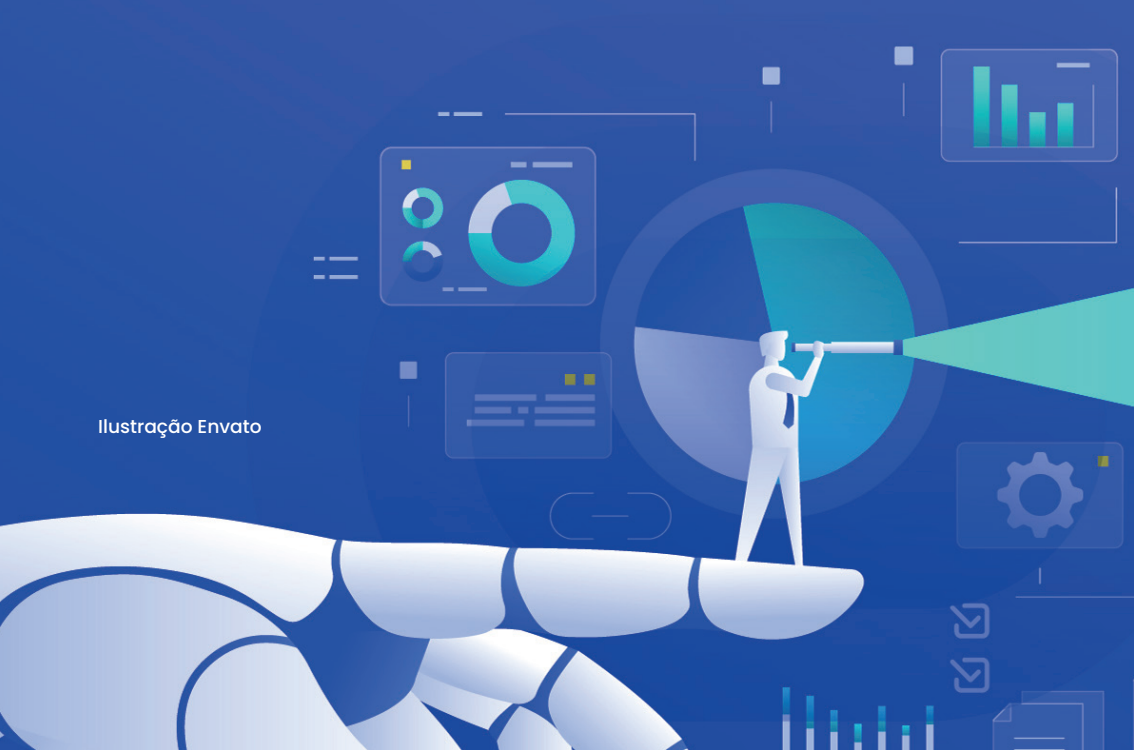


Ilustração Envato

INCIDENTES DE SEGURANÇA E SUSPEITAS:

- **Acesso e uso indevido a dados:**
  Caso você presencie ou tenha conhecimento de um colega acessando e/ou utilizando informações de pacientes ou de colaboradores sem ter a necessidade profissional para isso.

- **Perda ou roubo de dispositivos:**
  Se um notebook, celular, tablet ou qualquer outro dispositivo contendo dados pessoais for perdido ou roubado.

CUIDADO COM AS TENTATIVAS DE FRAUDE:

- **Mensagens ou ligações suspeitas:**
  Fique alerta! Pessoas mal-intencionadas podem tentar se passar por médicos, pacientes ou familiares para conseguir informações sigilosas. Sempre verificar a identidade de quem solicita informações, seja pessoalmente ou por telefone. Não forneça dados sem ter certeza da legitimidade do solicitante.

- **Tentativa de violação de acesso:**
  Golpistas podem enviar e-mails falsos (phishing), pedindo sua senha ou dados de acesso. Desconfie e não clique em links nem responda.

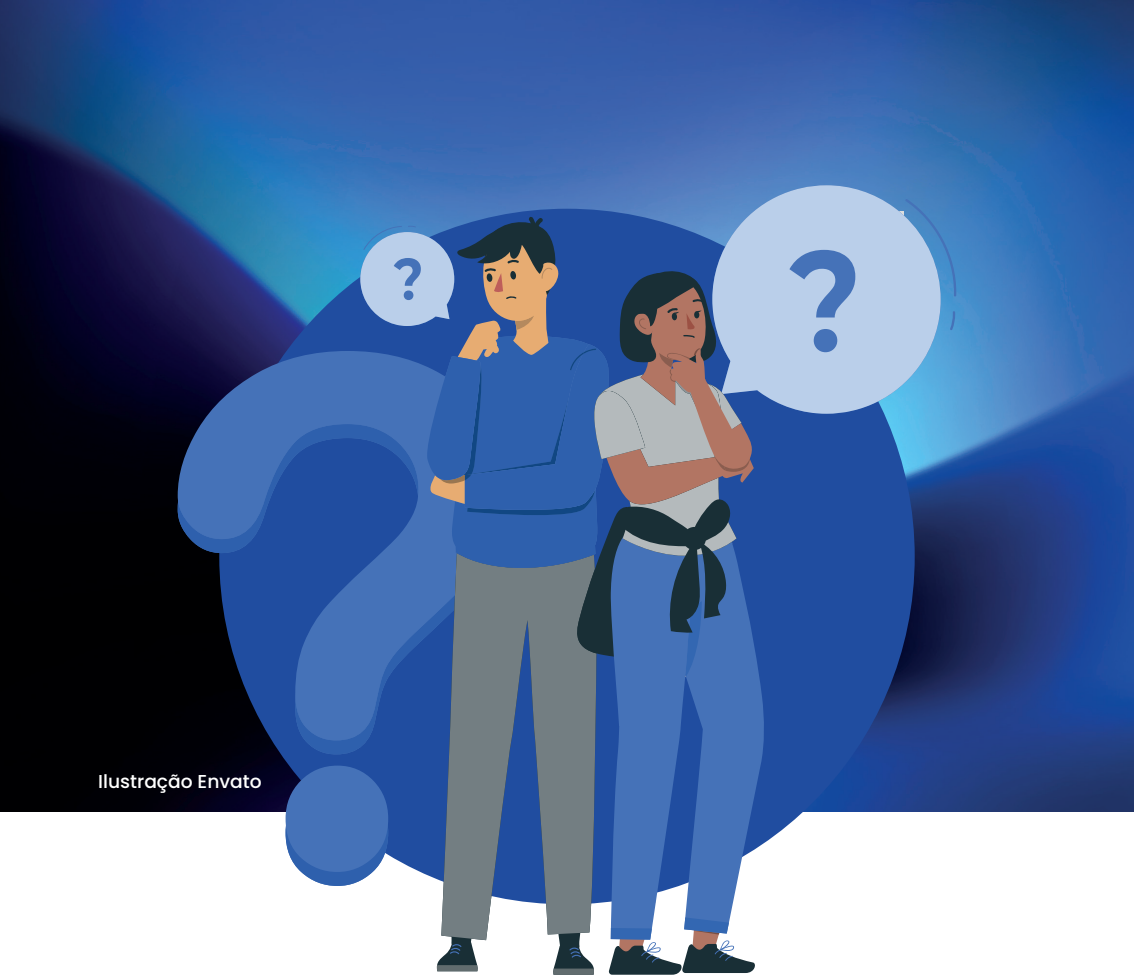


Ilustração Envato

DÚVIDAS E ORIENTAÇÕES

Lembre-se: É importante acionar a Equipe de Privacidade quando houver incerteza sobre **como tratar dados pessoais de forma segura e legal** em situações específicas.

Prevenir é sempre o melhor caminho para garantir a conformidade com a LGPD e proteger as informações de todos.

O HCP conta com uma página exclusiva sobre privacidade e segurança de dados, com conteúdos e canais de contato:
hcp.org.br/privacidade-e-seguranca

Lembre-se:
Você é um guardião dos dados.


HCP
anos
TRATANDO A VIDA
COM AMOR
HCP
GESTÃO