



## 10 formas de melhorar a segurança dos dados dos pacientes

Uma instituição de saúde, seja ela de pequeno, médio ou grande porte, lida, constantemente, com uma grande quantidade de pacientes. É responsabilidade do médico armazenar endereços, telefones e documentos, além das informações de atendimento, consultas e exames. Com isso, crescem os cuidados que devem ser tomados com esses dados, pois os pacientes esperam que eles estejam guardados de maneira segura.

Atualmente, estamos cercados por inovações tecnológicas, cada vez mais aprimoradas. Por isso, é praticado que uma instituição de saúde não utilize esses recursos para organizar os dados dos pacientes. O uso de computadores, internet e programas especializados no armazenamento de dados é um modo bastante eficaz para lidar com essas informações.

No entanto, por mais benefícios que essas tecnologias tragam, ao usá-las, estamos automaticamente vulneráveis a que informações pessoais sejam expostas ou caiam nas mãos de *hackers*. Em contrapartida, cada vez mais profissionais são disponibilizados para ajudar a fazer a proteção de dados importantes e confidenciais. Em função disso, o blog apresenta uma lista com dez medidas essenciais para manter seguros os dados dos pacientes.

### **Instale um bom antivírus**

Um dos elementos essenciais para manter a segurança de dados é a instalação de um antivírus eficiente. Ele oferece uma proteção contra *hackers*, pois dificulta o acesso deles ao sistema. Os planos de assinatura pagos oferecem uma proteção mais eficaz contra vírus e outras ameaças do que os gratuitos. Lembre-se que o antivírus deve estar atualizado para combater os dados com eficácia.

### **Crie senhas fortes**

Utilize senhas longas, compostas tanto de números como letras (maiúsculas e minúsculas) e caracteres especiais. É preciso ter uma senha diferente para cada local. Muitos cibercriminosos, após descobrirem uma senha, tentam acessá-la em outros serviços, pois muitas pessoas têm o hábito de repetir senhas. Isso facilita a vida dos *hackers* e dificulta a segurança dos dados. Portanto, altere-as constantemente.

### **Faça backup dos dados**

Também conhecido como cópia de segurança, o *backup* deve ser realizado com frequência. Isso permite que os dados sejam armazenadas em um outro local e dados importantes não sejam perdidos caso haja uma invasão ao sistema.

### **Sistema de autenticação dupla**

Este processo dificulta ainda mais o acesso dos *hackers* aos dados dos pacientes. Quando o sistema de dados

ativado, é necessário que, além da senha, um segundo código seja apresentado. Esse código pode ser enviado por celular, por exemplo. A autenticação dupla também pode ser realizada através do uso de biometria ou uma chave de segurança. Somente as pessoas autorizadas conseguem responder.

### **Criptografe os dados**

Basicamente, a criptografia faz com que os dados sejam visualizados apenas por indivíduos autorizados e que seja necessária uma chave para acessar tais informações. Isso acontece porque as mensagens são codificadas em um processo adaptado para a troca de mensagens on-line, permitindo que apenas o destinatário certo consiga ter acesso.

### **Cuidados no acesso ao wi-fi**

Dependendo das configurações da rede de wi-fi, o acesso de estranhos ao sistema pode ser facilitado. O protocolo WPA2 seja utilizado, reforçando ainda mais a segurança da rede sem fio. Além disso, se possível, disponibilize uma rede wi-fi exclusiva para visitantes, fazendo com que estes tenham acesso limitado à rede.

### **Treinamento dos funcionários**

Os funcionários que têm acesso ao sistema de dados devem ser bem instruídos, recebendo um treinamento adequado para que as falhas devido a fatores humanos sejam evitadas ao máximo. De nada adianta utilizar diversos recursos de segurança se as pessoas que lidam com o sistema de dados não sabem utilizá-los da maneira correta.

### **Evite links e sites desconhecidos**

Ao receber um link ou mensagem que considere estranhos, na dúvida, não clique. Muitos sites ou links, quando clicados, podem instalar programas maliciosos no computador que roubam senhas e dados pessoais. Se preciso, bloqueie cookies e scripts de terceiros considerados suspeitos.

### **Mantenha o sistema operacional atualizado**

A atualização do sistema realizada com frequência ajuda a manter os dados em segurança. Existem programas com atualizações automáticas, mas elas também podem ser feitas manualmente. O ideal é que exista um funcionário responsável por esta função, compreendendo as melhores maneiras de proteção contra possíveis ameaças.

### **Crie um plano de resposta**

Se todas as medidas de segurança falharem e os dados forem violados, é necessário estar pronto para reagir. Um plano de resposta preparado para resolver situações de crise deve estar disponível para lidar com um possível caso de perda de dados e informações.

Leia mais em: <https://docacademyblog.com>