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 gran
de pacientes. É responsabilidade do médico armazenar endereços, telefones e documentos, além das inform
atendimento, consultas e exames. Com isso, crescem os cuidados que devem ser tomados com esses dado
os pacientes esperam que eles estejam guardados de maneira segura.

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

No entanto, por mais benefícios que essas tecnologias tragam, ao usá-las, estamos automaticamente vulner
de que informações pessoais sejam expostas ou caiam nas mãos de?*hackers*. Em contrapartida, cada vez m
disponibilizados para ajudar a fazer a proteção de dados importantes e confidenciais. Em função disso, o blo
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. E
proteção contra?*hackers*, pois dificulta o acesso deles ao sistema. Os planos de assinatura pagos oferecem
contra vírus e outras ameaças do que os gratuitos. Lembre-se que o antivírus deve estar atualizado para co
dados com eficácia.

Crie senhas fortes

Utilize senhas longas, compostas tanto de números como letras (maiúsculas e minúsculas) e caracteres esp
preciso ter uma senha diferente para cada local. Muitos cibercriminosos, após descobrirem uma senha, tent
serviços, pois muitas pessoas têm o hábito de repetir senhas. Isso facilita a vida dos?*hackers?*e dificulta a s
de alterá-las constantemente.

Faça backup dos dados

Também conhecido como cópia de segurança, o *backup?*deve ser realizado com frequência. Isso permite q
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 d

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

Criptografe os dados

Basicamente, a criptografia faz com que os dados sejam visualizados apenas por indivíduos autorizados e q
?chave? para acessar tais informações. Isso acontece porque as mensagens são codificadas em um proces
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 ind
WPA2 seja utilizado, reforçando ainda mais a segurança da rede sem fio. Além disso, se possível, disponibi
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
para que as falhas devido a fatores humanos sejam evitadas ao máximo. De nada adianta utilizar diversos r
informações se as pessoas que lidam com o sistema de dados não saibam 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*, qua
instalar programas maliciosos no computador que roubam senhas e dados pessoais. Se preciso, bloqueie co
considerados suspeitos.

Mantenha o sistema operacional atualizado

A atualização do sistema realizada com frequência ajuda a manter os dados em segurança. Existem progra
atualizações automáticas, mas elas também podem ser feitas manualmente. O ideal é que exista um funcion
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 reag
preparada para resolver situações de crise deve estar disponível para lidar com um possível caso de perda
informações.

Leia mais em:https://docacademyblog.com