Você sabe como manter seus dados médicos seguros?

O dever de guarda dos prontuários médicos

Todo médico tem dever de guarda dos documentos gerados a respeito da saúde dos pacientes, os prontuários médicos. Durante a consulta o médico faz todos os registros necessários para a boa condução do caso e criação do histórico do paciente, e é responsável então por guardar esses registros de forma segura e apropriada.

O Conselho Federal de Medicina, na Resolução do CFM n.º 1.821/07 estabelece que os documentos médicos em suporte de papel devem ser arquivados por tempo não inferior a 20 anos, a partir da data do último registro de atendimento do paciente.

Com a era eletrônica e a necessidade de modernizar o meio de armazenamento de dados médicos dos pacientes, a Resolução 2.218/18 modificou a anterior, instituindo a possibilidade de se manter prontuários médicos somente em meio eletrônico, ou digitalizar os de papel existentes. Uma vez que o prontuário esteja digitalizado, ou sendo ele produzido em meio eletrônico desde sua origem, a guarda do mesmo não mais se limita a 20 anos, devendo ser permanente, como estabelece o artigo 7º da mesma Resolução.

Assim, para cumprir seu dever de guarda, é de extrema importância que o médico saiba como manter os dados seguros, adotando procedimentos que garantam a integridade e devido arquivamento das informações.

A segurança dos dados eletrônicos na era dos *ransomwares*

Os *ransomwares* estiveram bastante presentes nas notícias em 2021. Você pode ter ouvido histórias de ataques a grandes empresas, organizações ou agências governamentais, ou talvez você, como indivíduo, tenha experimentado um ataque de *ransomware* em seu próprio dispositivo eletrônico.

Ransom malware (*Malware* de resgate), ou *ransomware*, é um tipo de *malware* (ou software malicioso) que impede os usuários de acessar seu sistema ou arquivos pessoais e exige o pagamento de um resgate para recuperar o acesso.

Embora algumas pessoas possam pensar que "um vírus bloqueou meu computador", o *ransomware* normalmente seria classificado como uma forma diferente de *malware* e não de vírus.

As primeiras variantes de *ransomware* foram desenvolvidas no final dos anos 1980 e o pagamento deveria ser enviado por correio tradicional. Hoje, os autores de *ransomware* ordenam que o pagamento seja enviado via criptomoeda ou cartão de crédito, e os atacantes têm como alvo indivíduos, empresas e organizações de todos os tipos.

É um problema significativo e uma perspectiva assustadora ter todos os seus arquivos e dados mantidos como reféns até que você pague.

E como você pode ser infectado por um *ransomware*? Existem diversas maneiras, mas, em todas elas, primeiro o agente de ameaça deve obter acesso a um dispositivo ou rede. Ter acesso permite que ele utilize o *malware* necessário para criptografar ou bloquear seu dispositivo e dados. Algumas maneiras pelas quais um *ransomware* pode infectar seu computador incluem:

- Arquivos maliciosos enviados como anexos em um e-mail;
- Anúncios maliciosos em sites da web que redirecionam para servidores criminosos;
- *Phishing*, uma técnica de engenharia social que engana os usuários para obter informações confidenciais, fazendo-os clicar em um link malicioso.

Diante disso, para garantir que seus dados estejam seguros em meio às crescentes ameaças do meio virtual, você deve adotar práticas específicas que protejam seus dados e a integridade deles.

Práticas para manter seus dados médicos seguros

Em primeiro lugar é importante tomar todas as medidas possíveis para evitar que seus dados seja comprometidos de alguma forma. Isso inclui tomar diversos cuidados na navegação online, tomar cuidados com as redes acessadas e também cuidados com os equipamentos utilizados, por exemplo:

- Estar atento a links, e-mails, websites e propagandas suspeitas. Nunca clicar em nada que não tenha certeza sobre a procedência e segurança.
- Ao acessar um site, se for solicitada permissão para acessar sua localização, não permitir.
- Não permitir salvar seus dados de login nos diversos sites em que loga na internet, principalmente as senhas de acesso.
- Não permitir que o navegador faça downloads automáticos.
- Limpar os *cookies* do navegador periodicamente.
- Evitar o uso de extensões e complementos.
- Evitar o uso de redes Wi-Fi públicas ou desconhecidas para acessar seus dados.
- Desabilitar a configuração de conexão automática a Wi-Fi *Hotspots* em seus equipamentos.
- Manter antivírus e *firewall* ativados e atualizados.
- Evitar o download de programas e arquivos não relacionados ao trabalho em seu consultório, minimizando os riscos.
- Fazer as atualizações solicitadas pelos equipamentos, tanto computadores quanto celulares e tablets, pois as atualizações corrigem falhas importante e garantem a segurança dos equipamentos.

Além das medidas preventivas, que buscam evitar que seus equipamentos sejam infectados por vírus ou sofram ataques de *ransomware*, por exemplo, também é essencial adotar práticas de backup dos dados, garantindo que, ainda que você sofra algum ataque ou ocorra qualquer outra eventualidade, você terá uma cópia segura dos dados, de modo que eles poderão ser facilmente recuperados.

Backup dos dados: a melhor garantia para seus prontuários médicos

O backup é a garantia definitiva de que seus dados estão seguros e não serão perdidos em nenhuma circunstância. Isso se o backup for realizado da forma correta. Criar o hábito de fazer backup periódico dos dados é inclusive importante não apenas para os dados médicos do seu sistema, mas também para qualquer dado que você mantenha em seu computador, celular ou tablet e que não possa perder, incluindo documentos diversos, fotos, etc.

Assim, para manter seus dados seguros, você deve realizar periodicamente o backup local dos dados, salvando uma cópia deles em local seguro, e também realizar a sincronia diária dos dados com a nuvem, mantendo assim uma cópia dos dados online.

Neste ponto, é importante ressaltar o diferencial do software médico que funciona instalado em seu computador, em relação ao software médico que funciona apenas na nuvem.

Enquanto nos sistemas exclusivamente online seus dados ficam salvos apenas na nuvem, no software médico instalado (que também funciona online), você tem a real posse dos dados, uma vez que eles estão salvos diretamente em seu computador.

Isso permite que, além de fazer a cópia dos dados na nuvem, através da sincronia com os servidores online, você também possa fazer uma cópia dos dados locais, em uma mídia física, como um *pendrive* ou HD externo, duplicando o nível de segurança dos seus dados e mantendo total controle sobre eles.

Lembre-se que tanto o backup online, realizando a sincronia dos dados do computador com a web, bem como o backup em mídia física externa, devem se tornar um hábito e serem realizados com frequência. Se você fica uma semana sem fazer backup, por exemplo, caso os dados do computador sejam perdidos e precisem ser recuperados, os dados dessa semana que ficou sem backup não terão recuperação.

Backup dos dados no HiDoctor®

No HiDoctor® o processo de backup é simples e oferece dupla garantia aos médicos. Você pode realizar a sincronia dos dados, salvando uma cópia deles nos servidores da Centralx®, bem como pode copiar os dados salvos localmente em seu computador em outra mídia.

Como o processo de sincronia é simples e rápido, o ideal é realizá-lo diariamente, no fim ou no começo do dia.

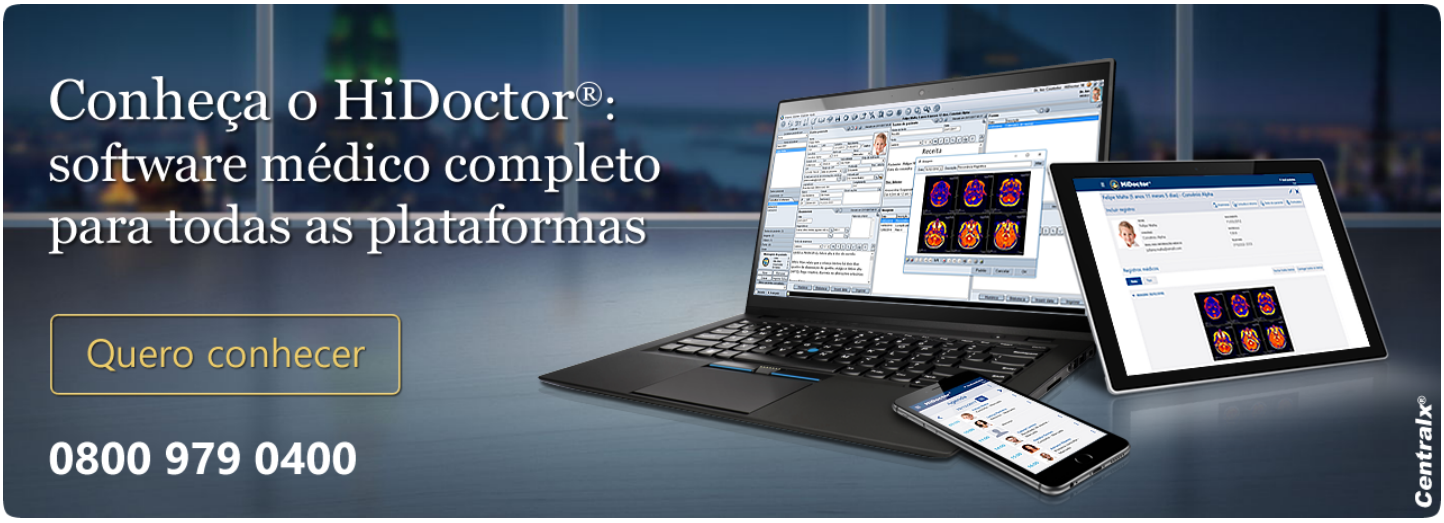
Ao fazer a sincronia, é oferecido também para fazer o backup local dos dados. Esse processo também é rápido e idealmente deve ser feito diariamente. É o arquivo que esse backup gera que você deverá copiar para uma mídia externa.

Todo o processo leva pouco tempo e garante que seus dados estejam sempre seguros.

» Veja como fazer o backup dos dados no HiDoctor®

O médico tem responsabilidade sobre o registro, a guarda e a segurança dos dados médicos dos pacientes. E o HiDoctor® pode ajudá-lo nisso, pois oferece a maior segurança para seus dados, permitindo que você tenha controle sobre eles e faça seu próprio backup, além de oferecer o backup online como uma garantia a mais de que suas informações não serão perdidas independente de circunstâncias adversas que venham a ocorrer.

O HiDoctor® é a única plataforma médica completa para seu consultório e o software mais utilizado por médicos e clínicas no Brasil. A Centralx® conta com mais de 30 anos de experiência no desenvolvimento de tecnologias para a área médica.



Artigo original disponível em:

"Você sabe como manter seus dados médicos seguros? " **- HiDoctor® Blog**

Centralx®