Cuidados que você deve ter com seu certificado digital

Em um cenário em que a tecnologia está cada vez mais presente na rotina dos profissionais de saúde, os certificados digitais desempenham um papel crucial na segurança, autenticidade e confidencialidade das informações médicas transmitidas eletronicamente.

Os certificados digitais são essenciais para autenticar a identidade do médico no meio digital, permitindo que ele emita prescrições digitais para os pacientes, assine os prontuários eletrônicos, etc. No entanto, é fundamental compreender e adotar os cuidados necessários para proteger e manter a integridade do certificado digital, evitando problemas.

A seguir você confere 8 cuidados que deve ter com seu certificado digital para utilizá-lo com segurança e eficiência, mantendo a confidencialidade das informações dos pacientes e garantindo a validade legal de seus documentos.

8 cuidados a ter com o certificado digital

1. Nunca emprestar o certificado
2. Não anotar a senha
3. Guardar o token ou smartcard em local seguro
4. Certificado A1 exige muito compromisso com a segurança
5. Certificado em nuvem apenas no celular e tablet
6. Se possível, opte pelo certificado A3 em mídia física
7. Atenção à validade do certificado
8. Se necessário, revogue o certificado

1. Nunca emprestar o certificado

Um certificado digital é pessoal e intransferível, portanto, nunca deve ser emprestado a outras pessoas, para nenhuma finalidade, sob risco de se envolver até mesmo em fraudes, caso a outra pessoa utilize seu certificado para autenticar documentos sem seu conhecimento.

No caso de certificados emitidos para pessoas jurídicas, pode ocorrer de mais de uma pessoa fazer uso do certificado nas rotinas de trabalho. Nesse caso, deve haver um protocolo bem estabelecido definindo as pessoas autorizadas a utilizar o certificado e as práticas que devem ser adotadas pelos usuários para manter o certificado em segurança.

2. Não anotar a senha

Anotar a senha de seu certificado no celular, em sua agenda ou mesmo em um papelzinho que guarda na carteira é uma prática que oferece riscos. Se alguém consultar sua agenda, tiver acesso ao seu celular, roubar sua carteira, enfim, encontrar essa senha de qualquer forma, poderá usar seu certificado em seu nome, caso consiga a posse do certificado.

Lembre-se também de elaborar uma senha forte e memorável. Ainda que a senha criada precise ser longa e com diferentes tipos de caracteres, é interessante pensar em algum sistema que faça com que seja possível memorizá-la com facilidade, assim não precisará anotá-la.

3. Guardar o token ou smartcard em local seguro

O certificado digital pode ser gravado em mídia física, um token USB ou smartcard. Nesse caso, além de proteger o token ou cartão do acesso por terceiros, é importante mantê-lo a salvo de avaria física e exposição a líquidos e produtos químicos.

Guarde-o com o mesmo cuidado que você tem com seus documentos de identidade ou cartão de crédito.

4. Certificado A1 exige muito compromisso com a segurança

O certificado A1 é um modelo que fica gravado apenas no computador do usuário, o que exige diversos procedimentos de segurança para mantê-lo a salvo do acesso não autorizado e, ao mesmo tempo, para mantê-lo sempre disponível.

Esse certificado exige o backup da chave, uma vez que, por lei, a única cópia do certificado A1 fica com o usuário (a operadora não pode ter uma cópia). Assim, é possível perder por completo o certificado em caso de avaria, roubo ou perda do equipamento.

É desaconselhado utilizar o certificado A1 no celular ou tablet por serem dispositivos mais passíveis de roubo e perda, gerando diversos inconvenientes caso caiam em mãos erradas. Nesse caso, opte por um certificado digital A3 armazenado em nuvem.

5. Certificado em nuvem apenas no celular e tablet

O certificado A3 armazenado em nuvem proporciona a praticidade de acesso de qualquer dispositivo, bastando instalar o aplicativo da certificadora no dispositivo para conseguir emitir assinaturas digitais. Contudo, esse certificado depende da internet e da disponibilidade da certificadora para funcionar, por isso não é recomendado confiar apenas no certificado em nuvem.

Idealmente, você deve utilizá-lo restritamente em celulares e tablets porque é a única opção disponível para esses dispositivos.

6. Se possível, opte pelo certificado A3 em mídia física

O certificado A3 armazenado em mídia física/token é o padrão ouro porque reúne segurança e praticidade para o usuário: pode ser usado em diferentes computadores; fica disponível apenas para quem possui o dispositivo físico e a senha de assinatura; pode ser guardado em segurança com o

usuário; pode ser usado independentemente da disponibilidade da internet e não pode ser copiado/clonado.

7. Atenção à validade do certificado

Você não precisa aguardar o vencimento do certificado para renová-lo: a maioria das certificadoras disponibiliza a renovação do certificado a partir de 30 dias para o prazo do vencimento.

O procedimento é mais simples que a emissão e geralmente consiste apenas em pagar a taxa de renovação e manter o dispositivo conectado durante o processo.

8. Se necessário, revogue o certificado

Por fim, se houver perda ou roubo do dispositivo com o certificado instalado (seja computador, celular, cartão físico ou token), ou qualquer suspeita de comprometimento que possa ocasionar o uso indevido do certificado, entre em contato com sua certificadora e solicite a revogação do documento.

Esse procedimento deve ser feito imediatamente e pode ser realizado online ou presencialmente.

Os certificados digitais já fazem parte da rotina de grande parte dos médicos. Ao adotar essas práticas, os profissionais de saúde podem utilizar seus certificados digitais com tranquilidade, aproveitando os benefícios da tecnologia sem comprometer a segurança dos dados e a confidencialidade dos pacientes, nem ter problemas legais por uso indevido do certificado por terceiros.

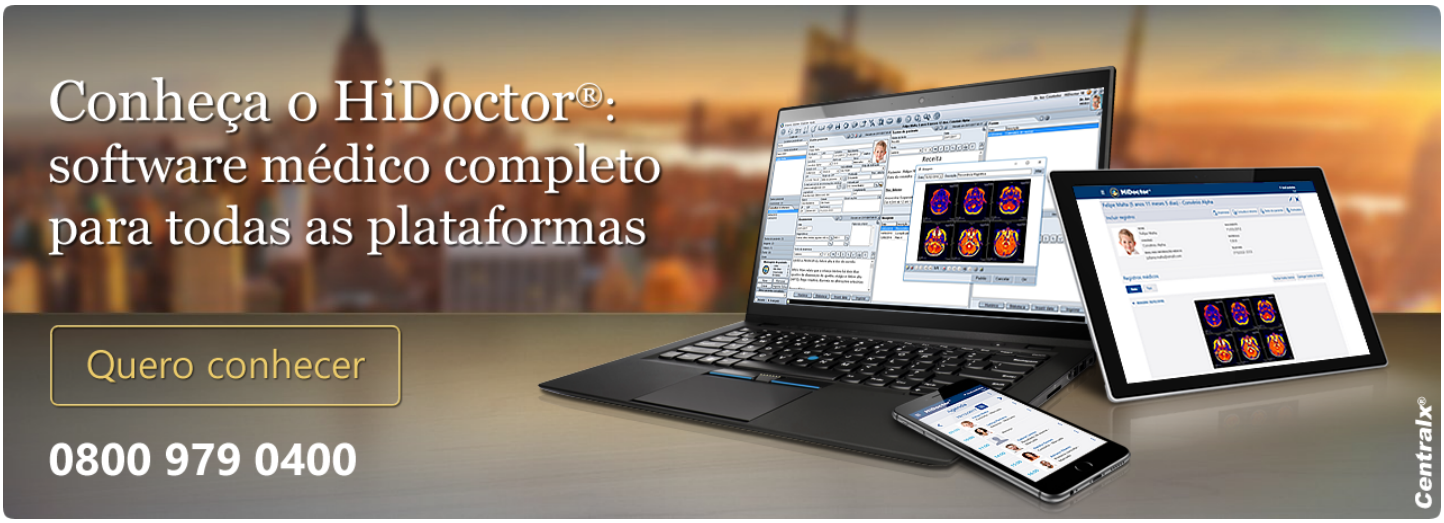
Se você deseja saber mais sobre a assinatura digital na prática médica, confira nossos outros artigos:

- Tipos de certificado digital – qual o melhor?
- Tudo sobre a assinatura digital dos prontuários médicos
- Assinatura digital – qual a importância e como usar no software médico?
- O que é necessário para emitir uma receita médica digital?
- Quais são os usos da assinatura digital para um médico?
- Diferença entre assinatura eletrônica e assinatura digital
- Glossário da assinatura digital – entenda todos os conceitos

No HiDoctor® você conta com assinatura digital integrada ao software médico, para simplificar a emissão de documentos digitais para os pacientes e a assinatura dos prontuários.

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.

Experimente e conheça clicando abaixo!



Artigo original disponível em:

"Cuidados que você deve ter com seu certificado digital " **- HiDoctor® News**

Centralx®