Codify
BY AAPC

Health Information Compliance Alert

Encryption: Follow These 5 Tips When Choosing An Encyrption Solution

Looking for an HIPAA encryption solution that works for your organization but doesn't break the bank? Whether you're trying to secure a small or large database, these tips will get you started in the right direction - and put a big smile on the face of your CFO.

Take a look at these tips provided by **Kevin Beaver**, president of information technology and security consulting firm **Principle Logic** in Atlanta.

1. MAKE SURE SOFTWARE SUPPORTS NATIONAL STANDARDS

Look for products that support Secure Sockets Layer and Transport Layer Security protocols as well as encryption algorithms such as Triple-DES and the recently published **National Institute of Standards and Technology**'s Advanced Encryption Standard.

Note: You can view the NIST's Advanced Encryption Standards at http://csrc.nist.gov/CryptoToolkit/aes/).

2. PURCHASE SOFTWARE THAT MAKES GOOD BUSINESS SENSE FOR THE SIZE OF YOUR ORGANIZATION.

A small physician office doesn't necessarily need a $15,000 appliance to create a public key infrastructure, and a hospital shouldn't rely on the digital signature features built into Microsoft Outlook.

Smaller organizations might not be able to afford an appliance for their network perimeter that costs thousands of dollars. There is often encryption software available for free with existing systems.

"[Covered entitites] can get digital certificates for virtually any e-mail client. They might have to pay a little for the digital certificate, but the encryption is built into the software. And with Windows 2000 and XP, they can protect the data at rest by turning on the built-in encrypting file system," says Beaver.

3. DON'T CUT CORNERS

If you're going to outsource encryption or buy an appliance to manage it, a well-established or name-brand product is the best option. The name-brand product might be a little more expensive, but you're not taking a chance with something you don't know. "It's never a good idea to try to cut corners and save money up-front."

4. CHOOSE AN APPROPRIATE ALGORITHM

A 64-bit encryption algorithm was cracked in 2002, so don't choose an encryption algorithm weaker than 128-bit, but don't go overboard, either. "128-bit encryption is really strong. More would be overkill," Beaver advises.

5. EDUCATE STAFF AND MANAGERS

Encryption can give a false sense of security. "All the encryption algorithms in the world can't prevent users from using a

weak password to digitally sign an e-mail or encrypt a hard drive."

Include encryption in security training and give anecdotal evidence to show staff what can happen when data is not encrypted. "And you have to keep management in the loop. Let them know what the industry standards are and what you're going to use," says Beaver.

The Bottom Line: Beaver says encryption should be part of a larger layered security infrastructure that includes firewalls, anti-virus software, user authentication, and appropriate access controls (see related story, "SECURITY"). When looking at your options, make sure you consider both data in transit - which includes any PHI that goes across an open network - and data at rest in a database on a server.