Health Information Compliance Alert

Security Compliance: Evade The Encrypted PHI Trap

Naiveté won't negate a security rule violation!

You've encrypted your patients' PHI. So, now what? If you think encryption removes PHI from HIPAA's radar, you could be setting yourself up for a violation.

Encrypted, Not Erased

Are you confusing the privacy rule's deidentification with the security rule's encryption?

Definitions: Deidentification is a method of ensuring patients' privacy by wiping their records of any identifiable information. After deidentification, the remaining content is useless. **Encryption,** on the other hand, is a security mechanism that obscures information from unauthorized users.

The difference? With encryption, "the information isn't gone, it's just made difficult to get to," explains **David Szabo,** a partner at **Nutter McClennen & Fish** in Boston.

Key Control

Though encryption does scramble PHI into unreadable segments, the puzzle can be put back together, experts say. And it's not hard. "A key is out there and encryption can be cracked or socially engineered," says **Fred Langston,** a principal consultant at **VeriSign** in Seattle, WA.

Ask yourself: "Who has the keys? Who stores the keys?" Szabo suggests. The fact that decryption keys exist mean that the encrypted PHI is vulnerable to privacy or security breaches and must be protected, Langston reminds.

Most important: Effective key management is crucial. Multiple key-holders are as risky as single ones, Szabo warns. **Tip:** Your office must determine who will distribute the keys and how many keys should be available.

And, "you don't want one person to hold all the keys to your encrypted information," Szabo advises.

Example: One company encrypted all its documents. The person in charge of that data died tragically. No one else had the key to that encrypted information and the organization had to spend time and money cracking the password.

Simplified Security

"Security is not just protecting information from unauthorized disclosure. It is also the protection of the availability and integrity of data," Szabo explains.

Ask yourself: "Does encryption answer the rest of my security obligations?" he suggests. "The fact that something was encrypted before it was destroyed in a fire does me no good. I still don't have it," Szabo says. If encrypted PHI is exempted from HIPAA's umbrella, then the same logic must apply across the board, Langston reminds. Therefore, "if I apply access controls to my patients' PHI on a secure server, then I could say that server no longer contains e-PHI," he says. "No one makes that interpretation, but it's the exact same argument."

The Bottom Line

Encrypted PHI remains protected health information, experts agree. "The information has not been removed; it still logically exists," Szabo says. Failure to apply HIPAA's regulations to encrypted PHI could spell disaster for your security

rule compliance efforts.