Health Information Compliance Alert

Security Tool: Encryption Policy Gives You The Keys To Wireless Security

Adapt this format to keep information thieves out and your PHI safe.

Encryption is your best weapon for locking unauthorized users out of the e-PHI you transmit over a wireless network or store on a wireless device.

Both during transmission and while at rest, e-PHI on your PDA, laptop or other wireless device is highly vulnerable to outside attack unless you take measures to conceal that information from all unauthorized users.

The following format, developed by HIPAAAcademy.net, can help you get started with an encryption policy for your organization that addresses the potential risks and lays out a solid plan for avoiding them.

ENCRYPTION POLICY

PURPOSE: To implement a mechanism to encrypt and decrypt electronic protected health information (e-PHI). The Encryption Policy is intended to assist employees of [Organization] when making decisions about the use of encryption technologies to protect data stored on systems that process e-PHI.

SCOPE: This policy applies to all [Organization] workforce members including, but not limited to, full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers and anyone else granted access to sensitive information by [Organization]. More specifically, this policy applies to employees of [Organization name] who have the authority to evaluate, purchase (or develop) and implement systems that store or process sensitive information such as e-PHI.

Further, the policy applies to all systems, network and applications, as well as all facilities, which process, store or transmit e-PHI.

POLICY: [Organization] will identify systems that require e-PHI to be encrypted.

[Organization] will identify members of the workforce who require encryption capabilities.

[Organization] will need to balance the challenge of protecting "data at rest" such as that defined in the Access Control standard of the HIPAASecurity Rule against the increased complexity of security technology and administrative overhead including performance considerations and usability.

[Organization] will seriously review the viability of securing critical database and file servers, as well as e-PHI on mobile devices such as laptops and PDAs.

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. Example: Network Associate's Pretty Good Privacy (PGP) uses a Layer (SSL) uses RSAencryption. Symmetric cryptosystem key lengths must be at least 56 bits.

Asymmetric cryptosystem keys must be of a length that yields equivalent strength.

[Organization]'s key length requirements will be generated will be securely escrowed.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Security Officer.

[Organization name] will test encryption and decryption capabilities of products and systems to ensure proper functionality.