Health Information Compliance Alert

Security 6 TIPS TO START YOUR SECURITY RULE COMPLIANCE

What's a federal regulation without controversy? Some say the answer might have arrived in the form of the final Health Insurance Portability and Accountability Act's security rule, but there are still some stumbling blocks covered entities must be on the lookout for.

While some covered entities may have been nervously awaiting ambiguous text or rigid requirements, the final HIPAA security rule startled many with an unexpected dose of flexibility. The Department of Health and Human Services Feb. 20 published the final security rule in the Federal Register , and most agree that the rule isn't unduly burdensome.

The security rule requires CEs to establish procedures and mechanisms to assure the confidentiality, integrity and availability of electronic protected health information. The regulation works hand-in-hand with the privacy rule standards and calls for CEs to "implement administrative, physical and technical safeguards" to protect electronic PHI.

While many of the original security rule provisions remain in the final reg, there are some notable changes including some potential pitfalls of which health care organizations should be aware. Here are some tips to keep in mind:

Know these four responsibilities. First of all, CEs must meet four major security requirements:

- Ensure the confidentiality, integrity and availability of electronic PHI the CE creates, receives, maintains or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such data;
- Protect against any reasonably anticipated uses or disclosures of such information; and
- Ensure compliance by one's workforce.

Rule applies only to electronic PHI. The final rule applies only to PHI in electronic form. Examples: Paper-to-paper faxes are not considered electronic, but computer faxes are, and voice telephone is not considered electronic, under the rule.

Reasonableness is defined. For those still perplexed over what are meant by "reasonable" precautions, the final rule actually defines what HHS considers reasonable.

According to the rule, determining what is reasonable requires a CE to apply a two-part test: the first step involves assessing the security risks it faces. Second, it must implement countermeasures proportional to those risks, as well as manage its countermeasures to keep up with new risks.

Flexibility = Scalability. All CEs are unique, and all have unique challenges when it comes to security rule compliance. The final rule is significant not only for what it includes, but for what it doesn't; in general, there are so-called "standards" that explain what CEs must do, and there are "implementation specifications" that HHS considers "addressable" (i.e., not essential).

These standards are grouped into administrative, physical and technical safeguards. For example, one administrative standard involves appropriate safeguards when dealing with business associates. If you communicate with business associates, the rule required you to have written contracts in place with the BA to ensure that BAs are charged with safeguarding the data that has been transmitted to them.

Additionally, the new rule is technologyneutral, meaning that the HHS doesn't require you to apply specific types of software to your security plan. That'll make security rule compliance a lot easier, and likely cheaper to boot, says Robert Markette with Gilliland & Caudill in Indianapolis. "For a lot of providers, for example, the flexibility to find a way to meet the standards on their own without having to use a specific kind of software makes compliance more affordable," he explains.

Document your physical safeguards. The rule calls on CEs to document all repairs or modifications to the physical components of their organization that relate to security. That includes putting locks on cabinets or doors that are easily accessible, if there's a risk that PHI could be leaked.

Example: A group of doctors at a large hospital didn't jump at the prospect of spending more money on new locks, says Richard Marks, an attorney in the D.C. office of Davis Wright Tremaine. Marks says people always have that reaction, but retorts, "some people don't like to have their cars inspected, but if you don't, you run a risk, and you have to accept that risk." Marks says another security tip to consider is to purchase a burglar alarm, preferably one with a motion sensor.

Markette agrees that documentation is key. He says it's important for CEs to have manuals documenting their security policies and procedures and any accompanying documentation." The reason is simple: If you document those policies and explain why you may not have implemented an addressable standard, the HHS Office for Civil Rights will have a hard time enforcing the rule against you in court, should it ever come to that.

Training is essential. The rule charges CEs with ensuring that security training is given to a CE's entire workforce, not only the part of its workforce that has contact with PHI.

"Generally speaking, everybody needs to be aware that they've got to keep information secure, and doing that is going to have an impact on everything they do and on all of their daily routines," Marks notes.

The effective date of the final security rule is April 21, 2003. Most CEs will have two years to comply with the rule, setting a compliance deadline of April 21, 2005, while small health plans will have an additional year before they're required to comply.

Editor's Note: The security rule is available in its entirety at http://www.cms.hhs.gov/regulations/hipaa/cms0003-5/0049f-econ-ofr-2-12-03.pdf.