Health Information Compliance Alert

Security Training: Take Good Care Of Your Phi

2 "reasonable precautions" you need to know about.

Are you certain you're handling your electronic health information according to the HIPAA rule's requirements? If not, it's time for a refresher or you could wind up with penalties and unwanted federal scrutiny. Review these fundamentals with your staff to make sure your security compliance is where it needs to be:

Application: The final security rules apply only to PHI that's in electronic format. That includes computer-to-computer faxes and e-mails. It does not include paper-to-paper faxes or voice telephone conversations.

Your Overall Task: You must take reasonable precautions to assure electronic PHI remains confidential, that the data remains intact and that the information is also available when needed.

Reasonable Precautions: What's reasonable depends on the circumstances. The final rule requires that you determine what's reasonable by:

(1) assessing the security risks you're facing and

(2) take steps to counter those risks and keep up with new risks that may arise.

Your Responsibilities: You have four primary responsibilities, all intended to prevent unauthorized access to PHI:

1. Keep all electronic PHI you create, receive, maintain or transmit confidential, intact and available whenever it's needed. **Example:** An information technology specialist should be on call 24/7 to resolve computer access and security problems.

2. Protect against all threats or hazards you can reasonably anticipate to the security and integrity (condition) of the electronic data. **Example:** Do not allow staff to share computer passwords. But do set up your computers with a "password-aging" program that would require your workforce members to change their passwords each month or so.

However, remember that the security rule is technology-neutral, meaning that the **Department of Health and Human Services** doesn't require you to purchase and apply specific software programs. "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," explains **Robert Markette**, an attorney with **Gilliland & Caudill** in Indianapolis.

3. Protect against any reasonably anticipated uses or disclosures of such information. **Example:** All computers with PHI should have an automatic log-off feature so that if you walk away from the computer, it will log off the current user within a given time. This will help keep any PHI from being left on the screen for anyone to see.

4. Be sure that your staff complies with the security regs. **Example:** Train and test staff on security measures, and monitor for compliance.

Document, Document, Document: You must document all repairs or modifications you make to physical security, such as putting locks on cabinets or doors that house PHI. It's important that you have manuals documenting your security policies and procedures and any changes you make, says Markette. The reason for all the documentation hassle: If you document those policies and explain why you may not have implemented a particular security standard, **HHS' Office for Civil Rights** will have a hard time enforcing the rule against you in court, should it ever come to that, he maintains.

Train, Train, Train: You have the responsibility for providing security training to your entire staff, not just those people who have 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," notes **Richard Marks**, an attorney in the D.C. office of **Davis Wright Tremaine**.