Securing Electronic HIPAA Data Becomes Hip

Stephen Barlas

Whether you work for a pharmacy, a managed care plan, or a health maintenance organization (HMO), if you are a pharmacist, two things are certain:

1. You are dealing with “protected health information” (PHI). This term, which is used in the Health Insurance Portability and Accountability Act (HIPAA), includes, among other things, prescriptions obtained by patients.

2. You are probably viewing the data on a computer screen near your desk. This information is “electronic” and is known as ePHI. It is subject to the dictates of the HIPAA’s security rule, which becomes effective on April 21, 2005.

So far, few people have heard about this rule. It is a “doosy” for employers, who will be responsible for deciding what kinds of ePHI protection policies to put in place, and for employees, who will become increasingly responsible for maintaining computer security (which they had previously thought was the job of information technology personnel whom they might encounter only if their computers had problems).

If your organization is not yet in the midst of a thorough risk assessment aimed at revealing computer security vulnerabilities, you are in big trouble. A risk assessment is the first step in complying with the security rule, but it is not a simple thing to do.

That was clear from the comments of several speakers at a conference sponsored by the National Association of Chain Drug Stores (NACDS) in early May. I will try to give you an idea of the level of angst that this security rule will bring to unsuspecting project managers.

Organizations will be required to appoint a “security official,” who will be charged with ensuring compliance. When someone from the audience asked Mike Griffiths, RPh, manager of pharmacy systems at Albertsons, Inc., whether his company had thought about hiring a consultant to run the entire process, he joked:

“After waking up at 3 a.m. a couple mornings in a row after getting this assignment, I started consulting with Jack Daniels.”

Mr. Griffiths designed the risk assessment for Albertsons. Because there was no actual template available, he created his own questionnaire by rummaging through the Web sites for the Center for Medicare and Medicaid Services (CMS) and the National Institute of Standards and Technology (NIST). He thought of 103 questions about computer and electronic data security vulnerabilities and the likelihood of specific threats to security.

He asked the survey takers—those employees at Albertsons who would be handling ePHI—to rank the probability and the potential impact of a serious threat to security. He then multiplied those two numbers to derive a risk quotient for each threat and each vulnerability.

“I was surprised at how much time it took to get those questionnaires completed,” he said. “I had to sit down one-on-one with some of our people and, in some cases, spend half an hour with them.”

The good part about the HIPAA’s security rule is its flexibility; a company can analyze the risks of, and the vulnerabilities to, the confidentiality, integrity, and availability of ePHI any way it wants. It doesn’t have to send out questionnaires. Keep in mind, too, that potential threats come not only from computers, as in the case of hackers; they can also be environmental, such as those involving malfunctions with water, electric, and heating systems.

Based on that risk analysis, a company can develop safeguards to address the possibility of viruses and worms and problems with computer log-in monitoring, password management, and the like. The rule takes into account the notion that a certain level of risk is acceptable. The operative words here are reducing threats to a “reasonable and appropriate level.” From there, pharmacies will establish training programs in each of these areas for their employees.

Deborah Faucette, RPh, director of pharmacy operations at the NACDS Foundation, emphasized that training can be done via computer, papers, videos, live sessions, or any combination thereof. After the initial training is completed, it must be reinforced and updated periodically, and those additional efforts must be documented.

Compliance with the ePHI security rule will affect all pharmacy personnel, and sometimes in ways you wouldn’t think of. So take those “sticky notes” with your passwords off those computer screens!

SUGGESTED READINGS
