

Three Myths About HIPAA Compliance

Overblown claims by software vendors and other misinformation can cloud the real issues involved in securing medical records.

R O B E R T C . F E I G H T N E R

The pending deadlines for compliance with the Health Insurance Portability and Accountability Act (HIPAA) have generated a cottage industry of consultants, seminars, and assessment and compliance tools. Numerous claims have been made about systems that will bring providers into compliance with the new patient information privacy and security rules.

Amid all of this information—much of it quite useful, it should be said—a number of “myths” have emerged that are clouding the issue at a time when providers are under great pressure to meet the pending HIPAA deadlines.

Below are three of the most common myths about HIPAA compliance.

1: “Our software will make us HIPAA-compliant.”

A facility’s software may be “best of breed,” but it can only be as good as the facility’s HIPAA policies and procedures and their proper implementation.

HIPAA compliance is a process, not a turnkey solution. The HIPAA security rules do mandate access controls and network and data-integrity protections. But the rules provide different examples of how to achieve these goals, and facilities will have to coordinate their HIPAA privacy policies with their information security procedures. Consider this hypothetical “bad example” (using a fictitious facility and vendor) of a good software system being undermined by poor security policies, procedures, and lack of HIPAA security-awareness training. “Swallow Point” is a long term care facility with a client-server software system. It has computer workstations on each wing. Swallow Point uses “Revector Systems,” an integrated

clinical-financial software system. Revector Systems advertises its software as being “HIPAA-compliant.” The software system contains the access controls that the HIPAA security rule requires, user identifications (IDs), passwords, and a timeout feature that shuts down user access after a predetermined period of time. These features, properly employed, would satisfy the HIPAA access controls under the proposed rule, according to comments in the *Federal Register*. Swallow Point did implement policies and procedures that require each user to have a unique ID and a password. However, it did not inservice the users on the importance of developing a secure password—one that is difficult to guess. Most employees use the names of their spouses, children, or pets as passwords. Swallow Point should have taught its computer users to develop passwords that are not common words, contain both letters and numbers, or that are unusual spellings of words.

The facility did establish a policy that each workstation must use a timeout setting of 15 minutes, but does not actively check whether users have reset the timeout period. Swallow Point’s management knows that many workstations have reset timeout periods as long as two hours, but does not address the issue in followup counseling. Also, the information technology (IT) administrator has set up an account with the ID “USERID” and with the password “PASSWORD” so that new employees, temporary employees, and employees who have forgotten their passwords can get instant system access if the IT administrator is not available to reset or administer system access.

It does not take a computer system security expert to know that Swallow Point’s

system does not provide any meaningful level of security. The software is not, in fact, “HIPAA-compliant.” If the Revector Software were properly administered in accordance with well-considered information security policies and procedures, Swallow Point could self-certify or obtain independent certification that it was HIPAA-compliant. But that compliance must be based on what the facility does across a range of functions, not merely the software it uses.

2: “HIPAA is not going to happen—at least not in my lifetime.”

You won’t hear health care leaders saying this any longer, but some rumors are still circulating. The effective date of the HIPAA electronic data interchange (EDI) rules was extended from October 2002 to October 2003 for parties that file a plan for extension. However, the extension of the EDI standards does not change the April 14, 2003, compliance date for the HIPAA privacy rules. And according to the sponsors of the EDI delay bill, Congress is unlikely to enact any other HIPAA delays. One co-sponsor of the extension bill, Rep. Thomas Sawyer (D-Ohio), said, “this is a one-time deal. We hope members will not come back again asking for further delays. The answer next time will be, I am certain, a clear and inarguable no.”

3: “The cost of HIPAA compliance will put me out of business.”

Performing a HIPAA assessment and implementing HIPAA-compliant privacy and security policies and procedures requires a substantial commitment of resources. It need not cost a fortune, however, and the HIPAA rules permit and encourage a facility to tailor its policies and procedures to its size and complexity. There are numerous no-cost resources available to assist a health care facility in learning the HIPAA rules and requirements (*see information box, page 64*).

More important than spending valuable resources and hiring cadres of consultants, providers should allocate adequate time and support to current facility employees to perform the HIPAA assessment and develop real-world policies and procedures. The first step in the process is to read the HIPAA regulations. The rules are long, but not impenetrable. When a facility's staff has a grasp of what the HIPAA rules mean, then the HIPAA assessment can begin.

A HIPAA assessment involves examining how a provider prepares, uses, and transmits patient information, and the technical and physical systems that transmit, store, and access that patient information. A HIPAA assessment will require an examination of the facility's information systems, a thorough look at the paper trail of a medical record, and a walk through of the physical plant to see who views what medical records where. Only after this as-

essment is performed, reviewed, and updated, if necessary, does the implementation begin.

Implementation is a four-step process, and combines the HIPAA rules and the results of the HIPAA assessment. Most providers will find that they are already following many HIPAA rules. Therefore, providers should document and reinforce in their HIPAA policies and procedures what the facility is already doing correctly.

Second, they should identify the areas where the facility is at risk and develop and implement remediation policies and procedures. Next, providers should thoroughly train their employees on the new policies and procedures.

Finally, after this is all done, providers should repeat the assessment and see what may have been missed. If HIPAA compliance is starting to look like a vicious cycle, it is because HIPAA is an iterative

process. It is never finished, but if done correctly, the facility gets better every time. ■

Robert C. Feightner, JD, LLM, is the HIPAA compliance officer for Achieve Healthcare Information Systems, Eden Prairie, Minn.

For More Information

■ Information on HIPAA can be found on the Department of Health and Human Services Web site at www.cms.hhs.gov/hipaa.

■ Other informative Web sites include: The American Health Care Association, www.ahca.org; the American Health Information Management Association, www.ahima.org; Health Key, www.healthkey.org; and the Association of American Medical Colleges, www.aamc.org.