Next Steps? First Steps? Getting a Grip on HIPAA Security Standards

Save to myBoK

by Anne Zender, MA

How ready are healthcare organizations to put the proposed security regulations connected to HIPAA into effect? What are the next steps-or, in some cases, first steps-HIM professionals should take? Our panel of experts offers some advice.

So you thought preparing for Y2K was a lot of work? To be sure, the industry's efforts to prepare for the century rollover were considerable. And there's more to be done as the implementation of HIPAA provisions looms. Some experts predict that the cost and effort to ensure systems are in compliance with these regulations will be even greater than the time and money spent preparing for Y2K.

HIPAA-the Health Insurance Portability and Accountability Act-was enacted in 1996 to streamline the processing of healthcare claims and reduce paperwork. As part of this legislation, in 1998 the Department of Health and Human Services (HHS) proposed a number of standards that would protect the security of electronic information. These standards would apply to all healthcare providers, plans, and clearinghouses. At this time, HHS estimates that the final rule will be released in May 2000. After that, providers will have a two-year window to become compliant.

How close are healthcare organizations in general to being ready to put the security provisions into effect? According to our panel of experts, not very. Though the proposed regulations have been released for some time, in many cases not much progress has been made. We asked a group of HIM professionals who specialize in regulation and security issues about some key HIPAA-related points and how HIM professionals can help lead their organizations in the race to the finish.

Our panelists are:

- **Pat Brown**, MS, RHIA, senior director, Middle Atlantic Region, HIS Division, QuadraMed Corporation
- **Ron Luetmer**, healthcare technology consultant specializing in small to mid-sized hospitals, Eide Bailly LLP, Fargo, ND
- **Jayne Lawson**, RHIA, information security manager, Hartford Hospital
- **Julie King**, RHIA, EMR director, University of Washington Medical Centers

Q. When the HIPAA regulations are finalized, facilities will have two years to put the proper measures in place. Which directives pose special challenges to HIM professionals? How can readers begin to prepare to address these?

Brown: Two of the major issues will be the ability to ensure that all information for the same patient is in one location in an electronic database and the digital signature. Many facilities have not performed a complete evaluation of the duplicate entries in their master patient indes (MPI), nor do they have ongoing monitors to correct and hopefully prevent errors in the registration process. HIM professionals need to take ownership for ensuring the integrity of the MPI so that one-to-one relationships exist for each patient's electronically stored health records. The digital signature definition provided by HIPAA is very specific and would eliminate the use of what many facilities currently call "electronic signatures," so HIM professionals need to lobby vendors to provide HIPAA-compliant digital signatures within the next two years.

Lawson: I agree that authentication will be an issue, and we'll also have to look at privacy standards. HIM professionals need to educate themselves about public key infrastructure and how it is tied to role-based access. Privacy standards will also be a challenge, especially to states that have established privacy and confidentiality laws. Determining when federal law will supercede state law, and vice versa, will be a challenge in itself. Many states may have more stringent laws and others, none at all. States that have to deal with out-of-state requests for information will be challenged with explaining how their state law supercedes the federal.

King: Two other areas to watch are policy and procedure development and audit logging and reporting. As far as policy development goes, there are many good resources available, including articles published by AHIMA and the CPRI toolkit. In terms of audits, HIM professionals will need to work with their IS departments to draft user requirements in this area. Again, they need to communicate these requirements to vendors so they can provide the necessary tools.

Luetmer: More generally, I think that education will be a challenge for HIM professionals in small to mid-sized hospitals. HIM directors must help their colleagues understand how susceptible electronic health information is to exposure. They generally have good, documented policies on handling paper records, but electronic data is handled with less supervision, primarily because people don't understand how information flows within computer systems. Small hospitals that until recently did not run a network for e-mail or have Internet access are rapidly catching up and implementing these tools. As they do so, the focus tends to be on the functionality of the system rather than the security risks. The first step to developing the right security policies and technical controls is a risk assessment identifying all the areas where health information can be leaked, accidentally copied, e-mailed, and so on. As a facility becomes networked, it must be stressed that security of electronic health information is not just the responsibility of the HIM director and IS director. It is everyone's concern.

Q. Healthcare facilities have had some time to assess the existing guidelines, even though final regulations haven't yet been issued. How have you been using the existing directives and applying them?

Lawson: We've used existing directives to develop our information security policies, standards, and guidelines. We will review any new directives against our existing policies to make sure we are in compliance.

King: I work within the information systems department of my organization. We have studied the guidelines, reached some consensus on interpretation, and developed a gap analysis of the requirements we need to focus on. We've also assigned a point person to identify the specific projects necessary for compliance with the standard. In addition, we have used the guidelines and related projects to determine budgetary needs and additional staffing requirements.

Brown: The guidelines are helpful when reviewing current and new software contracts. Asking vendors questions concerning HIPAA compliance is a good way to ensure that they, too, are also addressing the issues. If a vendor does not show interest or has not addressed the issues, I would doubt their ability to comply with the guidelines. I have heard stories of vendors who claimed their products were Y2K ready, but did nothing proactive until the last minute, resulting in many hours of stress and expensive "quick fixes" because it was too late to go to another vendor.

You can use the guidelines to bring attention to HIPAA issues. I use any opportunity to mention HIPAA when appropriate, such as when a medical records committee wants to install electronic signature software to decrease delinquent records-does it meet HIPAA's definition? When someone installs intranet "browsers" to facilitate use of a clinical information system, I ask if they provide audit trails (many do not) to meet HIPAA's guidelines. Desktop security is another question I often raise-how do we know that a user has not shared her password with someone else?

Q. In general, what is your impression of healthcare facilities' state of readiness? How close are people to being up to the standard?

Brown: Many hospitals, even though they are aware of HIPAA, have not even begun to assess their risk. They spent last year on Y2K preparedness. But most facilities won't even know how much work is to be done until they complete their risk assessment.

Lawson: I agree that facilities are nowhere near ready. But these standards will have a major impact on the exchange of health information, and facilities need to begin addressing the issues now. The two-year window that will exist once the regulations are finalized is a time frame for facilities to become compliant-not to start thinking about being compliant.

Luetmer: Smaller providers have been reluctant to do anything until the final regulations are issued. They see HIPAA more as a threat to an already tenuous bottom line than an opportunity to save billions of dollars through administrative simplification. They view complying with HIPAA as an IT expense, and smaller hospitals already spend a smaller percentage of their budget on information technology than a large metropolitan hospital. Because providers want to stretch their IT budget as tightly as possible, the knee-jerk reaction has been to hold back on committing resources if the rules of the game change with the release of the final regulations.

Smaller facilities are beginning to take their first steps, however, as they learn more about HIPAA and realize that the sooner they begin implementing the regulations, the more effectively they can manage an information systems strategic plan.

Q. What are the next steps people should take to get closer to where they need to be?

Luetmer: A gap analysis identifying the scope of the compliance project is the first place to start. While a 26-month compliance window may seem like a long time, the sooner you start, the better off you are going to be. Also, because the rule is scaleable to accommodate facilities of all sizes and since specific technologies are not mandated, evaluating a facility's compliance can be subjective. It would seem logical that, in an audit of practices once the regulations become enforceable, facilities that took a proactive approach would fare better than those that put off compliance efforts until the very last minute.

Lawson: I'd say that facilities need to do two things educationally: one is designate staff to become educated on the effect the regulations will have on their facility. The second is to engage upper management so that they provide support and dedication-to make sure of facilitywide cooperation. These are both areas where HIM professionals can make a difference.

King: One interesting facet to HIM involvement in this process may be that in many organizations, HIM professionals seem to be partnering with IS staff to determine necessary projects. This is yet another opportunity for HIM professionals to spotlight their expertise and contributions.

Brown: As we talk about contributions HIM professionals can make, we have to remember that we need to begin by educating ourselves. On an individual level, everyone can visit the HIPAA Web site (http://aspe.os.dhhs.gov/admnsimp/) and read professional publications on this topic. The next step is to find a logical committee structure within the organization (maybe the same structure or group that handled Y2K issues) to be the focal point for distributing information concerning the assessment. This group should perform a risk assessment and begin to plan corrective action as soon as possible.

Q. How can facilities assess their existing systems and make sure that they are up to regulation?

Lawson: One way to begin a risk analysis is to develop checklists based on what the proposed regulations require. Use the checklists to perform a risk analysis to see where the gaps are. Communicate with vendors of your current systems to make sure they are working to be HIPAA compliant.

King: As you look at systems, work with members of your security team to develop an assessment tool. In a large organization, enterprise applications are easiest to assess first. You can then develop assessment tools for departmental system owners to use on applications they have some "ownership" in.

Luetmer: Vendor communication is critical. You need to understand what your vendor is and is not responsible for. There are a lot of variables to consider here, too-for example, Y2K pushed some vendors with small client bases and limited resources out of the market. For the rest, HIPAA compliance will be an even bigger challenge than the Y2K fixes were.

Depending on a facility's contract with its vendor, these updates may or may not be covered by a software maintenance fee. It would surprise me if most vendors did not pass on at least some of the cost for HIPAA compliance to their customers. I'd ask vendors to put in writing the scope of what they plan to do to meet the regulations. If your health information network consists of multiple systems, don't assume that just because each of your vendors say they are going to comply with HIPAA that the sum of all those parts meets the regulations. Systems should be audited by a third party who fully understands HIPAA and can evaluate all of the systems in the facility to make sure security is up to par.

And remember that a large percentage of HIPAA compliance work falls outside the scope of your systems vendor, including the development of administrative, physical, and technical procedures to safeguard patient-identifiable information.

Q. Why is it important for HIM professionals to be key players in the process of getting up to speed with HIPAA? How can they ensure that they are players at the table?

Lawson: HIM professionals have always been patient advocates when it comes to privacy. They have also been the trained professionals when it comes to coding. HIPAA will have a direct impact on functions that we have performed in the "paper world" for years. Our expertise is vital to take these concepts into the electronic environment that HIPAA is mandating.

Brown: That's true. HIPAA places more emphasis on the "rules of the game" for the 21st century. Therefore, we-HIM professionals-need to become experts on it. Learn as much as possible about HIPAA and be among the first at your facility to propose an educational session for key hospital staff concerning HIPAA. Volunteer to lead a HIPAA task force and be vocal about your knowledge of security and data transfer. And help other hospital departments assess their risk for HIPAA compliance.

Luetmer: HIPAA is important because HIM professionals have traditionally been the leaders in safeguarding patient information. While existing policies regarding the management of paper records may be airtight in a given facility, the same information existing in electronic media may not. HIM professionals need to fully understand the relative ease with which this information can be duplicated and delivered across a network so the issue receives the attention it deserves.

King: I believe HIPAA presents us with a lot of opportunities. For example, HIM professionals interested in security positions can learn from the more "technical" staff and be introduced to security challenges. But generally, although many of the standards are quite technical in nature and require more technical expertise for assessment and solutions, others are more administrative in nature and require expertise, such as HIM skills, for interpretation and problem solving. Bringing these skill mixes together-technical and administrative-provides a more complete solution.

Authentication-Getting Personal

The proposed rule for security requires that facilities have in place a mechanism for "entity authentication"-ensuring that users are who they say they are. This mechanism ensures that access to information is controlled and prevents unauthorized people from accessing data. The proposed rule mandates an automatic logoff and a unique user ID. A system should also include one of these features to authenticate users:

- biometric features
- password
- PIN
- telephone callback
- token

Whether you choose a simple or high-tech solution, you'll need to observe some fine points. Our experts offer these tips:

- While user ID and password is the most common authentication method, ensure that it is being used appropriately. Avoid use of "common logon IDs" such as "nurse" for viewing patient records at a nursing station
- Sharpen your knowledge about secondary authentication options. How can you determine what secondary authentication measures are necessary for your applications?
- Consider moving toward enterprise-wide authentication, in which a single and unique logon identifies the user in all of the systems he or she can access
- Determine what policies exist in your organization regarding authentication. Are new policies or revisions to existing ones necessary? Are people following the existing policies?

A Handy Tool

Some of our panelists recommended the Computer-based Patient Record Institute (CPRI) Toolkit: "Managing Information Security in Health Care," as a handy tool in the compliance process. AHIMA has contributed a considerable amount of information to this resource, including information security-related practice briefs and articles from the *Journal of AHIMA* and *In Confidence*. The kit is available online from http://www.cpri-host.org/, or call (301) 657-5918.

Access Controls-In Case of Emergency, Break Glass

Access controls, according to the proposed rule, restrict access to resources and protect communications over networks so that they can't be intercepted by anyone other than the intended recipient. This mandate presents some administrative challenges, particularly in designing policies and procedures that grant different levels of access to different people. Physical access to information needs to be considered as well. The proposed rule also requires a procedure that requires emergency access. What are the options, and how can HIM professionals help their organizations choose the best mechanism? Our experts offer some advice.

- Start with the basic rule that access to health information should always be on a "need to know" basis. Determine security levels with specific guidelines. Avoid pitfalls such as group passwords
- Develop an access matrix that determines, at a minimum by staff role, what desired access levels should be
- Establish short but reasonable timeouts for terminals used to access health information. Carefully consider, too, where these devices are located-high-traffic areas may present problems
- When choosing an access control system, look for one that assigns protection levels to individual data elements within each directory or file
- Become knowledgeable with access control levels offered by vendor-supplied products. Identify categories of "sensitive patients" that may require additional access controls. What would desired controls be for these patient categories? What appears to be the regional standard in some of these categories?
- Remember that access controls should not interfere with critical and timely access to patient information. Make sure that an override exists for emergency situations-for example, to give a physician access to medical history that he or she may not normally have access to in case of an emergency

Audits-a Watchful Eye

Identifying data access activities, assessing security, and diagnosing system weaknesses-all of these can be accomplished by audit controls. The proposed rule requires facilities to establish an audit mechanism that records and examines system activity-a feature frequently discussed in conjunction with alarms and event reporting. Audit controls can include in-house reviews that monitor logins, file accesses, and security incidents. Our panel offers some ideas for key steps to ensure that your facility has met the requirement.

- Create a written policy and procedure for ongoing monitoring of access to health information. You may want to monitor the records of certain types of patients (physicians on staff, dignitaries, mental health patients, etc.) periodically
- Choose a statistically valid sample of staff to monitor on an ongoing basis, especially those with high-level access rights, such as those within the HIM department. The important issue is to monitor the access and provide reports of the monitoring as needed
- Look at monitoring of access and access controls together; both are necessary for a more complete picture of needs
- In many cases, further development or vendor requests for functionality are necessary to meet the audit requirement. Don't underestimate the time this may take
- Before launching audit processes, make sure policies and procedures are in place to deal with potential breaches of information that may surface. Also, inform staff and be prepared to educate them on the new process
- Make sure your audit process is an active one. Users should be aware that audits are conducted frequently and at a certain level of detail, so that they know their actions are being monitored. Make sure there are sufficient obstacles to breaches of confidentiality such as authentication and authorization-and sufficient deterrents, such as a well-advertised practice of frequent audits and threats that misbehavior will be observed. But remember that if there are too many obstacles that prevent providers from getting access to the information they need, they will stop using the technology altogether

Assessing Your Risk

Our experts recommend performing a risk analysis as a first step to measuring your facility's level of compliance with the HIPAA security regulations. To brush up your risk management skills, you might want to consult these and other resources:

Collins, Patricia. "Risk Management 101." *Journal of AHIMA* 70, no. 9 (1999): 32-34.

Carroll, Roberta, ed. *Risk Management Handbook for Health Care Organizations*, 2nd ed. Chicago: AHA Press, 1997.

"Risk Management." Chapter in *Health Information Management Practice Standards: Tools for Assessing Your Organization*. Chicago: AHIMA, 1998, pp. 173-188.

Anne Zender *is editor of the Journal of AHIMA. She can be reached at mailto:annez@ahima.org.*

***Article citation**:*

Zender, Anne. "Next Steps? First Steps? Getting a Grip on HIPAA Security Standards." Journal of AHIMA 71, no.4 (2000): 27-32.