Wrestling the HIPAA Security Regulations: Two Experts' Advice

by Steven Austin

HIM professionals know they need to prepare for HIPAA, but where should they begin? Take a lesson from your peers at two of the nation's leading healthcare facilities.

HIM professionals know that the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is demanding a near transformation of the healthcare industry. What may not be clear, however, is how they should be preparing for it. We spoke with the HIM directors at two of the nation's leading healthcare institutions about pending HIPAA regulations and what they are doing to ensure their facilities meet them. Donna Bowers, RHIA, is director of HIM at Baylor University Medical Center and D'Arcy Myjer, PhD, is director of HIM services for Stanford Hospitals.

What Works for Data Security

Q: Do you favor restricted access to information or open access with audit capabilities?

Myjer: I don't see it as much as a personal preference issue as it is working within the cultural context of the institution for which you work and advocating for security. It is a little bit like solving simultaneous equations. What you're trying to do is find the solution for all the equations at once. Security is just one equation in the matrix, and your goal is to find a rational balance between protecting patient confidentiality and the ease of doing business. The position you end up taking has to balance regulatory requirements, the culture of the institution, and the strength of the administrative leadership.

The fundamental effort at Stanford has been on audit control: giving controlled access with back-end auditing. For example, a user must have a reason to be on the system, that is, the right to know, and his or her access is determined by job position. Once managers establish access, the employee is given a user ID and can establish a password that changes at regular intervals.

We haven't restricted access to a particular patient or a particular unit. We find that patients and physicians move too quickly for anyone to keep up with them. However, we conduct retrospective audits to ensure that each access was appropriate; that is, the employee had a need to know. At Stanford, we are experimenting with different audit approaches. These include:

- choosing a day and auditing all access for that day
- choosing a small number of patients and following them through the entire registration, treatment, coding, and billing cycle
- having a primary care physician review all access to several of his or her patients
- asking a department manager to review all accesses by his or her department for a randomly selected day

Bowers: Baylor's position is very much like Stanford's. We are not supportive of open access. We feel there must be some restrictions put in place up front. An example would be the ability to determine roles and relationships when attempting access to patient information. If a physician acted as an attending physician or a consultant on a particular case, when he or she attempted to access that patient's electronic health information, the system should be able to determine that there was a role relationship. If so, the physician could gain access to the needed information. If no role relationship could be determined, then the physician or other user would be denied access to the electronic health information, and some other party would determine whether the physician or other healthcare provider could gain access.

However, the restrictions can't be so cumbersome that physicians will not use the system, so there have to be some limits. We haven't found a solution yet. Rather, the vendors haven't found a solution yet.

Most of the vendors handle security one way or the other. We feel the auditing process is critical and we have had to perform audits several times. I can't see Baylor ever going toward open access, because we take a very strong stand on protecting patient confidentiality, even among healthcare providers including physicians. There has to be a legitimate business or clinical need to access a patient's medical record, and we are faced with this issue every day. When researching and implementing a new computer system, access is generally at the top of the functionality list to review and is always given a high priority.

Q: Are you working on procedural issues regarding restricted data access? For example, do you have security policies that include punitive measures for people who violate policy?

Bowers: About two years ago, a team developed the Baylor Health Care Systems Data Policy. When developing the data policy, no other models were used because none were really available. Baylor contacted several prestigious organizations around the country to determine if others had already done this particular development. Baylor did not want to reinvent the wheel if it could be avoided.

Unfortunately, no other organization had a program that could be used as Baylor's model. The outcome of the team effort was a document that addressed ownership of data (including patient data, physician data, financial data, research data, quality data, and personnel data); release, confidentiality, and security of data; and even went so far as to delineate some procedures for the organization. Previous to this, we really did not have anything in writing at a system level. All of the HIM departments had policies and procedures regarding release of patient information, but those policies and procedures did not include other types of data such as physician data, employee data, financial data, and research data. It took us about two years to draft this document and get it through the proper approval channels. That was our foundation, and I can't tell you how many times we have gone back to that document when we have had security issues. While it does talk about disciplinary action and so forth, it is a very broad document.

Now we are in phase two: the development of our security policies. We have a different team working on developing policies regarding electronic signature, using the Internet and e-mail at work, and transmission of patient information across the system. Those are things that will be included in the security phase.

Myjer: In many ways, the Stanford approach is similar. To answer the question of whether or not we would fire someone [for violating security policies], the answer is yes. We have specific policies that say if an employee violates security, there will be disciplinary action up to and including termination. The policies are written so that there is some management discretion. For a flagrant violation there can be immediate termination. For others, a warning is issued. We follow up on potential violations, and we have found that you don't need very many occasions for people to pay very significant attention. Regarding policies, we have adopted a similar approach. We started with a security plan about two years ago that mapped out the waterfront, and we've been working steadily on defining and refining policies.

No Time Like the Present

Q: How should healthcare enterprises be preparing now for HIPAA? If facilities have not taken the approach that both your institutions have taken, what should they do first?

Bowers: HIPAA has been around for quite some time now. However, because the regulations are far-reaching, many people within organizations are not familiar with the privacy components. To ensure that everyone, or at least key individuals, were up-to-date, we brought in an outside consultant to meet with HIM, our compliance team, and corporate counsel. The consultant reviewed the HIPAA regulations with us. Our goal is to educate the administrators and others so that we can then seek their support and the needed resources for an appropriate structure and processes to adequately handle these new requirements.

Myjer: In lots of organizations, some work has been done already. It is just a matter of mapping out what exists and integrating that in a single structure. My first answer is that people should read the rules: go to the Internet and actually read the rules before reading everyone else's distillation of the rules. There is often a difference between what is claimed to be there and what is actually there.

My other recommendation is to form a security committee that reflects the key players within the organization: hospital administration, the clinical side (physicians, nursing, and ambulatory care), the HIM and IT side and the major supporting departments (patient financial services, risk management, legal, and human resources), and ancillary departments (lab, pharmacy, and radiology) that control much of the information and data within the hospital. Administration should also appoint a manager responsible for security for the institution, so that there is a single executive who is ultimately responsible for assessing risks and accomplishments.

Take an assessment and act on the obvious things you can do. An assessment should focus on policies and procedures, technical network security and firewalls, back-ups and disaster planning, patient confidentiality policies, physical security of paper charts, shredding of paper printouts, location and time-outs of PCs, issuing of passwords, access audits, and training and education. The longer-term requirements will fall into place after you have done some of the immediate items.

Write policy and security plans. You can do them in either order, but building a security plan first gives a macro view, which allows you to move to more specific policies.

Stay customer-focused. The regulations are clearly designed to protect patients both when they are being treated and in the long-term use of data thereafter. Remember the patients' rights and needs as you develop policy.

Remember that **security is more than just a technical component.** Some institutions get into a "security equals information technology" mindset. Yet when you read the regulations, much of what is being discussed is not specifically information technology-oriented. There is, however, a strong component that is IT-oriented, including firewalls, technical disaster, and recovery plans. But the general issues of access and use of information are bigger than information technology.

Limit and audit access at the same time. It is a two-pronged approach: determine who has access to what information and what they are looking at. Limiting access requires that the institution decide and write down who has a right to access what type of information-based on job title, position, person, unit, or department. However, a right to access does not mean an employee has a need to know about any specific patient. So audit control looks at whether the access was needed and appropriate.

Develop a continuing program of training. If you are going to ask people to comply with your security perspective, you have to tell them what it is and what constitutes a violation. Stanford's solution is to train at multiple points. We train all employees during orientation and we also ask each department head to retrain as part of their ongoing yearly training plan within the department.

Finally, reassess. Once you've gone through all the entire cycle, then it's appropriate to start again.

Q: There seems to be a sense that from an administrative view, the HIPAA security regulations are going to require more effort than Y2K. Is that a true sentiment?

Bowers: No, I would put this on the same level as the fraud and abuse initiative. Y2K was a temporary issue, albeit an important one. HIPAA will be important but will have implications for many years down the road. It is going to be a very serious matter for hospitals that will cost far more than the Y2K initiative. I think Joint Commission will be monitoring very heavily for this in the future, along with other accrediting and licensing bodies. I have heard that this will become a new area of focus for them.

Institutions have spent hundreds of thousands of dollars, if not millions of dollars, developing compliance programs, and with HIPAA, I think they will do the very same thing.

Myjer: I think [the administrative effort required] depends on where you are and how much progress you've made. If there has been effort over the last several years, security will not be nearly as overwhelming. The issue is bringing it all together. It's just like Donna's point about the compliance regulations: it's not that we were not paying attention to coding or the accuracy of coding before, but now we put coding into a larger framework and there are larger consequences for not doing it right.

HIM Professionals: Stand Up or Take Cover?

Q: Will the regulations change your role as an HIM professional or the profession in general?

Bowers: From my perspective, I think HIPAA only provides more career paths for the HIM professional. At Baylor, HIM gets called upon for advice and support regarding many of the compliance issues. HIM led the initiative on developing a data policy and is providing leadership in the area of data security. HIM and information services are working very closely together in this area. Any time a department wants to install a new system, use electronic signature, or do anything with patient access or retention of data, they come to HIM for advice pertaining to the development of their policies and procedures. Our professional outlook is very positive for those who have an interest in this area. The skill sets that most HIM professionals possess are ideal for this particular aspect of regulation development and enforcement.

Myjer: Any time there is a change in regulations, there is an opportunity. If the HIM profession doesn't grab it, someone else will. This is a chance to say, "This belongs properly within HIM." The question is, at a personal level, is security of interest to you? Second, can you make the time, both personally and within your job priorities, to add it to what you are doing?

There are several things one can do. Become a member of security committee, and if possible, chair it. Develop security as a job category within the HIM department; develop the personal expertise that is required to talk appropriately to the issue; learn the appropriate technical language; and develop a large-scale picture. For example, compliance isn't just about coding; it is a much bigger statement about acting ethically. Similarly, when thinking about security, think about that at the CEO, COO, and VP level, not just in terms of the HIM department.

Q: Have security officer positions been created in your departments?

Myjer: We created one at Stanford under the HIM department, but then with the merger [with the University of California at San Francisco], that position was moved to the corporate level. Since the split of the two organizations, we have not yet recreated this position. The optimal person would have several skills: political acumen and security advocacy (within the medical center and with our vendors), the ability to translate regulatory awareness into concrete, feasible plans, policies, and actions, and an understanding and appreciation for the technical issues.

Bowers: At Baylor, there are two security positions. Both positions call for RHIA credentials with a preference for a master's degree as well. They are responsible for all the security in the databases within HIM, plus the physician databases throughout some of the system, as well as the MPI, and, potentially, the enterprise MPI.

We have also started a HIPAA task force, though it's still in the early stages. However, I believe that we will end up naming a security officer as well as a privacy officer. I think the security officer will be embedded in the IT structure and organization, while the privacy officer will be embedded in HIM. At this point it is too early to tell whether these will be new positions or if the responsibilities will be added to existing roles.

What Does HIPAA Mean for the CPR?

Q: Will HIPAA security regulations make implementing a CPR harder or easier?

Myjer: I think the issue of security is really a larger societal question about individual privacy. We all give away a lot more information about ourselves than we did 30 years ago. Business efficiency has argued that we share even more. On the one hand, each of us, as consumers and members of society, worry about what others know about us. Organizations want more information, whether it is to make our healthcare system work better or make their marketing campaign more effective. At a societal level we are saying, "Wait a minute! I think maybe organizations know too much about me, it's too integrated, and in the wrong hands it could be dangerous." What is going on with the HIPAA regulations, and what's going on in general, is the issue of personal privacy. HIPAA is not just about the fact that the federal government is making rules. They are making rules for a reason.

The HIPAA security rules are substantial. The challenge for organizations will be to put that together. Some of us have done lots of security stuff, but we haven't codified it into policies. Others write policies but don't have good enforcement of the policies. Others focus on one set of policies, but have not been as aggressive with other issues. The trick will be to bring it all together and do all the required paperwork.

In terms of a step forward or backward, it depends on how much of a bite there will be to the penalties-that is, how much will the federal government, the Joint Commission, and the state actually punish us for doing things wrong? For example, compliance works because the federal government levies substantial fines based on its findings. HIPAA will probably slow down some of the more aggressive computer projects. Security will be more of a factor, and project owners will have to spend time thinking "Is the security really there? Do we really believe the vendor?"

It is easy to say that a system presents a secure environment, but is it secure in all of its connections, not just within itself, but in all of its interconnections-inside and outside of the organization? My sense is that HIPAA will make us think more, and if thinking means slowing down, then maybe that's a good thing.

Bowers: I think HIPAA regulations will make the implementation of electronic medical records more difficult. However, I think that it should be made more difficult so that everyone involved will take the time and proper measures to ensure patient privacy. Many of the vendors that I have seen have built these systems around the open access viewpoint and I think the state laws have been very lackadaisical in protecting patient confidentiality. This, of course, is the reason HIPAA was conceived to begin with. If the state isn't going to deal with the issues appropriately, then the federal government will step in and take over, and that is what we are currently experiencing.

Society is becoming more knowledgeable about rights to privacy with regard to medical information. Society has also become aware of the lack of privacy that really exists in healthcare and, as a result, people are becoming vocal that too much is known about individuals. Pressure is now being placed on everybody to tighten all the rules. Without a doubt, I think tighter rules are needed, because too much information is getting out to too many people, and individuals are becoming afraid to tell their physicians their true medical history in fear of what harm can be done by a breach. It will eventually affect the quality of care if people are afraid to talk to their physicians. So I think HIPAA is a good thing. It will impede us a bit, but in the long run, we will all be better because of it.

Steven Austin *is a writer for SoftMed Systems, Inc., based in Folsom, CA. He can be reached at* mailto:saustin@softmed.com.

Article citation:
Austin, Steven. "Wrestling the HIPAA Security Regulations: Two Experts' Advice." *Journal of AHIMA* 72, no.2 (2001): 41-44.