Journey of 1,000 Miles: Are Providers Really Ready for HIPAA's Privacy Requirements

Save to myBoK

by Mark Hagland

Healthcare leaders say there's no time to waste on serious compliance work, and HIM professionals will be at the heart of the action in this area.

Eunice Little isn't nervous about HIPAA. After all, she and her colleagues at UCLA Medical Center in Los Angeles are in the small minority of healthcare provider organizations that have made significant steps toward compliance with the soon-to-be-finalized privacy and security provisions coming out of the passage of the Health Insurance Portability and Accountability Act of 1996, universally known by its acronym, HIPAA.

Intended to reassure healthcare consumers of the confidentiality of their personal health information, HIPAA is hitting the healthcare industry like a tidal wave, now that its privacy standards have been made final. But a small number of provider organizations, as well as health plans and insurers, have moved forward despite uncertainties about the legislation's privacy/security aspect (the electronic transaction standards were finalized during summer 2000, and, according to many in healthcare, transactions work is far ahead of privacy work, both at provider and health insurer organizations). And those organizations have already learned lessons that could be helpful to everyone else in the industry as providers struggle forward through a sea of details and questions.

For Eunice Little, RHIA, UCLA's director of health information management services, the path toward HIPAA compliance has been relatively straightforward, given the complexities involved. The HIPAA process at UCLA began in late 1999 with the formation of a steering committee to establish a planning process with three broad tracks of development-education, assessment activities, and the development of polices and practices. All three have made significant progress to date, but no one at UCLA, least of all Little, is underestimating the challenges ahead.

"The challenges here relate to the comprehensiveness of this," Little reports. "The scope involves not just hospital information systems, but the operations of departments and manual processes. The various things that can be included in the scope of the assessment are the biggest challenge."

In fact, she reports, working through policies and practices has turned out to be a broad and complex endeavor, confirming what industry experts have been saying all along-that developing HIPAA-compliant policies and procedures will be an "ongoing effort" well into the future, as she puts it.

Part of the key to the success of the process at UCLA so far, says Michael McCoy, MD, UCLA's CIO, is pulling together the right combination of people. "I think the combination of the chief compliance officer and the director of HIM services, that's the right team to put together" in terms of HIPAA compliance leadership, McCoy says, adding that of course the overall team must be broad and multidisciplinary.

And, despite the challenges of privacy/security compliance under HIPAA, McCoy says that, given the right kinds of planning, leadership, and follow-through, success is possible in this area, despite dire warnings to the contrary. "You hear a lot of 'HIPAA's going to be like Y2K,' and I think that's wishful thinking on the part of consultants," he says. In fact, he notes, "We're doing an inventory and an assessment of what we need to do," and proceeding apace.

"HIPAA's a many-faceted regulation, and some of the security stuff required in the regulation we already do," McCoy says. The key, he says, is for provider organizations to start now to make progress in this area. While HIPAA compliance is doable, it's far broader and more complex than many realize.

Working toward HIPAA compliance will also impact HIM professionals, though neither McCoy nor Little believes that it will fundamentally change their roles within provider organizations. "This isn't so much a big challenge internally within HIM services as it is a challenge in terms of planning how information flows in and out of that operation," Little says. "For most people working in that area, their jobs will appear to be the same. But I do see lots of work to be done on policy and procedures and in managing changes to information flow in that area." Training and education are key areas, too, she notes.

Industry Experts Agree on Urgency

If HIPAA seems like a difficult nut to crack, it's primarily for a few reasons, industry experts say.

First, hospitals and other healthcare provider organizations have spent years simply waiting for the outcome of the final privacy/security standards to be known, rather than moving ahead to prepare for anticipated standards.

HIPAA Privacy Standards Compliance: Advice from the Experts

Industry experts and professionals at provider organizations working on the privacy and proposed security requirements under HIPAA say provider executives, managers, and clinicians need to consider the following:

- Begin the process of inventorying your organization's data situation immediately. This is a months-long process in itself, says everyone who's done it
- It may sound self-evident, but read the Federal Register information on HIPAA. Much of what is being passed around as received wisdom is just that, in regard to HIPAA specifics
- Focus on HIPAA as a business process issue, not simply as an information technology or medical records/member records issue. All those involved in HIPAA work now say the real challenges have to do with realigning business and operational processes-information technology is a part of the challenge and solution, but only one significant part among many
- In that regard, say those in the trenches, it's absolutely vital not only to have complete support and buy-in from the very top of the organization, but also to have the very active involvement and participation of staff from all affected areas across the organization--information technology, medical records/HIM, medical management, nursing, call centers, legal affairs, regulatory affairs, public data reporting, and so on
- A key area that is only beginning to be dealt with so far is that of contracted vendors, such as those companies to whom healthcare organizations have outsourced pieces of their data and IT operations. This area, say experts, could become contentious and certainly is
- Many experts advise creating an organizational leader on HIPAA issues, but, they quickly add, this HIPAA "czar" or "czarina" needs to report directly to the very top of the organization, not be kept locked away in some remote department. He or she needs a lot of visibility, as well as the funding to make good decisions and move the compliance initiative forward
- Whoever is in charge needs a dedicated staff for the organization's HIPAA initiative, experts urge, though which types of individuals might be on that staff is an question that is still under discussion
- Funding is emerging as a major challenge--both coming up with the funding to prepare for HIPAA compliance and gauging actual costs. Provider organizations involved in the process report that it's very difficult to determine a concrete price tag for HIPAA preparation, but everyone agrees it will be costly over time
- Treat this as a doable process, much like a compliance program for Medicare or Medicaid fraud regulations, for example
- Consultants may be able to help frame the issues for your organization, but ultimately, moving into compliance with the HIPAA privacy and security standards will require the kind of thorough, attic-to-basement evaluation and realignment of business and operational processes that will necessitate intensive internal work

significant in regard to the potential civil and even criminal penalties for incidents of non-compliance with HIPAA privacy/security standards. A very thorough review of outside vendor contracts alone will be a major component for most healthcare organizations in moving toward compliance

anyway. In other words, say those in the know, this is not something that can be "handed off" to external consultants to "take care of"

- Think about HIPAA strategy in terms of your organization's overall e-commerce and e-health strategies as well

Second, HIPAA privacy/security compliance involves planning, action, and attention to detail across a broad range of areas, operations, and activities. Unlike, for example, Y2K, HIPAA preparation will require multidisciplinary collaboration across entire healthcare organizations. And, precisely because it is so broad, and because it speaks to the inventorying of organizational operations at such a detailed level, HIPAA preparation cannot simply be handed off to consultants or performed by a single department or group of staff members at an organization, say experts. In fact, experts offer a long list of dos and don'ts that they say health system executives and managers must consider very carefully in order not to fall into major pitfalls along the way toward compliance (see "HIPAA Privacy Standards Compliance: Advice From The Experts," above).

Where are most healthcare provider organizations right now? Not very far along, say experts, who are urging providers to move now to attain compliance.

"The first step is to assess where your organization is today in relation to the regs," urges Greg Hedges, a partner in the technology risk consulting division at Arthur Andersen in Chicago.

"The devil is in the details on HIPAA," Hedges says. "For example, sanctions are required for breaches of security. Well, what does that mean? Will you have to fire individuals for specific types of activities? Most organizations are looking at this at too high a level, and I would recommend to the CEO at an organization that the security and privacy officers identify specific gaps. Many organizations aren't even doing that yet. At a minimum," he adds, "you need to assess what your risk points are in the information flows of your organization, whether you're an insurer or provider." And, he says, organizational leaders should fear less that their process will have to be modified in the face of the final privacy regulations and more that they won't be giving themselves enough time overall to work on compliance, a much more likely scenario.

"I'm finding that organizations tackling this are doing at least a cursory look at their systems on the technology side, around passwords, networks, protocols, that sort of thing," says Keith MacDonald, a senior manager in the emerging practices group at First Consulting Group, Boston. "And though unfortunately healthcare has always had difficulty funding information technology, organizations are now starting to look at advanced technologies that will make log-ons easier for doctors, for example." HIPAA, MacDonald says, is giving healthcare organizations an opportunity to begin implementing advanced technologies like swipe cards and bioinformatics applications like thumbprint-based identifiers.

At the same time, he says, providers will have to deal with considerable training and education issues for staff and clinicians and will have to work through vendor/business partner relationships and contracts. A key step in this direction, he says, will be initiating the time-consuming process of reviewing and revamping policies and procedures, many of which will have been often inconsistent across care sites and even within care sites in organizations.

"If you have anything going on with the Joint Commission, a lot of the standards there on information management are very much the same as under HIPAA, including privacy requirements," McDonald says. Meanwhile, he says, "You've got to catch third-shift people, and you've got to engage physicians who might not necessarily understand the importance of this." HIM professionals will play a vital role in the educational and training aspects of that process.

And, despite the complexity and the tremendous amount of time, energy, and staff resources involved, Arthur Andersen's Hedges says part of the key to success will be to "leverage off resources you already have." Smart organizations, he says, are reutilizing their Y2K project teams under a different guise, with senior IT people, top HIM professionals, legal staff, and physician leaders among the key players this time around.

Providence Leverages Its Y2K Resources

One organization that is following that type of strategy is Providence Health System, a Portland, OR-based integrated health system. There, inventorying has been completed, and a team of HIM professionals, IT managers, clinicians, and others is working through policy-and-procedure work and other activities.

Explains Rita Aikins, the system’s information security/privacy officer, "We took what we did for Y2K and basically used that as a baseline and built from there, in terms of the technology inventory." As for the process aspects, Aikins says, "We looked at what we did for Y2K, but this project and Y2K are not one and the same. And so we aren’t managing this the way we managed Y2K."

One major difference between the two situations, she says, was that it was possible to approach Y2K remediation globally across her organization’s care sites in four states (Oregon, Washington, California, and Alaska), whereas differences in privacy and security policies and procedures are such that HIPAA compliance preparation can only be approached on a statewide basis.

Still, even though "patient and member mix is a little bit different in each state," Aikins is able to report that the overall process for HIPAA privacy preparation is similar throughout the system. She and her colleagues have a formed a project team, which she says is working along multiple tracks. The team is working to complete the risk assessments for each facility and has expanded the process to look at the organization’s business practices more broadly, with individual department assessments being carried out under the umbrella organizational assessment. And though the organization has its own health plan, she says that Providence Health Plan has its own designated HIPAA project manager. Given the differences between HIPAA preparation on a health plan level and a provider level, though, "where it makes sense, things are shared," she adds.

One important point, Aikins notes, is that once Providence managers had developed their risk assessment tool during the year 2000, they piloted the process at one hospital and found that a great deal of the process had to be modified for the broader assessment process to work organization-wide. In that regard, she says, it’s clear that time is the most valuable resource in HIPAA compliance preparation. And though large organizations like hers may have more human and financial resources than smaller ones, they’re also generally far more complex, she points out.

Kaiser’s Nationwide Effort

That observation would certainly not be lost on Mary Henderson, national HIPAA program director at the Kaiser Permanente health system/health plan. With hospitals, medical groups, and health plans operating in 11 states and the District of Columbia, few would question that the Kaiser organization is facing a massive challenge in HIPAA compliance preparation, even as it moves forward with a highly ambitious electronic health service program nationwide.

"This is very complex," says the Oakland-based Henderson, "it affects a lot of our organization, and so it requires a very distributed ownership. And we are a set of health plans, a set of medical groups, and hospitals in three of our regions." Not only that, but in contrast to Y2K preparation (which Henderson helped lead at Kaiser as well), "the issues are those that pertain to the actual provision of care, which is interesting."

And though the Kaiser organization’s EDI/transactions work is already far along, a solution having been proposed and implementation proceeding, work on the privacy side is still relatively recent, though now moving into high gear. To date, Henderson reports, "We’ve read the proposed regs, developed a security matrix, and scoped the regs." In addition, the organization is implementing a public key infrastructure (PKI) along with the implementation of its new national clinical information system, and linking work on the PKI with progress on HIPAA compliance.

Meanwhile, HIPAA leaders have been designated for each region, and planning is proceeding toward the development of a full risk assessment for the nationwide organization. And as at the other organizations interviewed for this article, Henderson says HIM professionals will be critical to helping Kaiser achieve HIPAA compliance because of their expertise in handling patient-confidential information.

Henderson also echoes others in saying that her key piece of advice is to get going now on HIPAA, "because the clock is ticking. And get good sponsorship from people at the highest levels of the organization who know what HIPAA is and what we have to do, fund the process, and remove barriers." She says she also has to remind herself that, given the many competing priorities in her organization, she, as a HIPAA leader, has to be able to articulate the need for compliance as a priority.

As at UCLA and Providence, Henderson says she and her colleagues at Kaiser are confident that they'll meet the two-year requirement for compliance, following the publication of the final HIPAA privacy standards. But she remains worried about some out in the field. "I was at an industry meeting the other day," she reports, "and they asked us to raise our hands if we thought we'd be compliant in time. I raised my hand, but not many others did." Now is not the time to panic, she says; "I don't think panic is productive, anyway. But if one doesn't get going quickly, they may be in a panic situation."

Mark Hagland *is a Chicago-based independent journalist and public speaker in healthcare. He can be reached at MHagland@aol.com.*

Article citation:
Hagland, Mark. "The Journey of 1,000 Miles: Are Providers Really Ready for HIPAA's Privacy Requirements?" *Journal of AHIMA* 72, no.2 (2001): 28-32.
