Busier than Ever: Privacy Officers One Year Later

Save to myBoK

by Ruth Carol

The HIPAA privacy rule implementation is a year in the past. So what are privacy officers doing with all their spare time?

In the long, hectic months leading up to April 2003, privacy officers were preparing their organizations for the implementation of the HIPAA privacy rule. Not only was the rule new and uncharted, so was the job. Now, with the implementation date a year behind them, how are privacy officers faring? They are busier than ever.

While the initial implementation of the rule—designed to protect and guard against the misuse of individually identifiable health information—is long over, privacy officers have the ongoing challenges of staff training as well as auditing and monitoring for compliance. They serve as their organizations' HIPAA experts, investigating potential breaches of privacy reported by workers and patients, and they assist their security colleagues with the next phase of HIPAA, which goes into effect April 2005 for most covered entities.

"I'm much busier after April 14 than I had expected to be," says Nancy Vogt, RHIT, CHP. Vogt is manager of privacy compliance and chief privacy officer at Aurora Health Care in Milwaukee, WI, an integrated delivery system consisting of 14 hospitals, 85 clinics, 135 retail pharmacies, two nursing homes, and a home health agency with 11 branches. "When I first took the job, it looked more like a project. But there's still a lot of refinement and improvement that has to be done, in addition to investigating patient complaints."

The biggest hurdle that Vogt had to overcome was "distributing the right information to the right groups of people," who, in this case, were spread out across approximately 400 facilities. To accomplish this task efficiently, she developed a network of 26 implementation coordinators at key sites. "It would have been impossible to learn all the patient access and HIM people at each site," says Vogt.

Same Law, Different Entities

One of the biggest challenges privacy officers face is applying the rule across the many different components that comprise their organizations. These days, Vogt spends her time trying to maintain consistency and standardization regarding the privacy rule while maintaining some flexibility among the varied entities in Aurora Health Care. "We want to have consistency in how we interpret the privacy law, with some tweaks that will work for each of the environments of care," she says.

Vogt is not alone in this task. Assuming the privacy officer position in January 2003, Kaye Monello, RHIA, CHP, executive director of HIM at Tallahassee Memorial Healthcare in Florida, had to learn the regulation quickly. Then she had to determine how the law applied to the different components within the 770-bed organization, which provides acute care, inpatient and outpatient behavioral health services, skilled nursing and home healthcare, a family practice residency program, and four family practice clinics. "I had an understanding of the big picture of the procedures and practices in the different settings, but I had to come up to speed very quickly in terms of the details to address where we had compliance and risk issues," she says.

Paula J. Richardson, RHIA, privacy officer and HIPAA coordinator for Wake County Government in Raleigh, NC, had to make the rule applicable to all of the health services the county provides, including mental health, social services, and public safety. "I had to create policies and procedures that were generic enough to be adapted by 50-plus public and private agencies," she says. Because most of the services are contracted out, Richardson was also responsible for educating and training her own staff as well as those at the various agencies.

Train, Audit, Monitor

Training, auditing, and monitoring are ongoing challenges being met by privacy officers on a daily basis. "In the beginning, my job was to ensure that the gap analysis occurred and the high-risk areas were taken care of before April 14," recalls Chana Feinberg, RHIA, director of medical records and privacy officer at Mount Sinai Hospital of Queens in Flushing, NY. "Now, it's the auditing to make sure that the different departments are complying. The auditing is extremely extensive and the training constant."

Often that training has to be tailored for staff at the affiliated entities, or even departments within the same facility, and then monitored to determine its effectiveness.

If available, many privacy officers employ electronic means to tackle these tasks. Vogt, for example, developed the training for 24,000 employees over a three-month period, relying heavily on the organization's internal Web resources that could track when individuals completed the training. She also provided a paper-based version of the training for the approximately 2,000 staff members who did not have access to computers.

Currently Vogt is working on a comprehensive compliance plan. Having identified 13 areas in which staff are not applying the rule correctly, she is building a network of compliance coordinators to conduct audits at their respective sites. Vogt is also creating a Web-based program that will remind managers when audits are due and allow them to complete the audits online. "Then I can spend my time tracking and trending the results and not on monitoring," she notes. Finally, Vogt is creating an educational tool to address questions she commonly receives. "I'm beginning to see patterns of what people don't understand," she says.

More than HIPAA

Privacy officers not only have to keep up with HIPAA, they must stay current on relevant state laws, which can be more restrictive than the federal regulation. State requirements may be imbedded in several laws, making them more difficult to track.

Laura Manley Knoblauch, MBA, RHIA, assistant director of health services and privacy officer at Illinois State University in Normal, is caught between HIPAA, state laws, and the Family Education Rights and Privacy Act (FERPA). Student medical records are typically covered under FERPA, whereas nonstudent records, such as those of faculty and staff, are covered under HIPAA. Just one of the dilemmas is what to do with records of students who are also faculty or staff members. If the university follows HIPAA for all records, it could be in violation of FERPA, and vice versa.

If that's not confusing enough, now come the state laws. Student records that have been solely maintained by the healthcare provider and never released to anyone are exempt under FERPA and covered under state law. "It's an administrative nightmare," says Knoblauch, who as cochair of the American College Health Association's HIPAA task force has contacted the Department of Education and the Department of Health and Human Services about the conflicting privacy standards. No official response has been received, but she was told that the two offices are discussing the problem, which affects all colleges and universities that treat both students and nonstudents.

Meet the Public

Responsible for investigating potential breaches of the rule, privacy officers are interacting more with the public than in the past. Investigating practices or incidents reported by employees or patients and then figuring out how to handle the situation if a violation has indeed occurred can take up as much as a quarter of a privacy officer's time.

"When a patient complaint comes in, it's an immediate priority," says Vogt. "If we respond in a timely manner, we can address the issue internally and keep the patient from going to the Office of Civil Rights."

In addition to handling patient complaints, Wendy Mangin, MS, RHIA, director of medical records at Good Samaritan Hospital in Vincennes, IN, receives calls from patients who want to correct or amend their records. Mangin also implemented a process for asking patients if they want to be included in the facility directory. "We have to explain that if they say no, it means they

won't receive any telephone calls, visitors, mail, or flowers," she says. Mangin had to train staff on how to explain the rule to patients and even developed a script to do so.

Far-reaching Advice

Privacy officers have increased their role throughout their organizations. Knoblauch has more interaction with other departments that provide healthcare on campus, and she works more closely with upper management, including the university president and vice president of student affairs. When she wanted the university to approve a policy related to the privacy rule, she had to go through several councils.

Adds Monello, "I didn't realize how far reaching the privacy officer's responsibilities would be." She now works with more upper-level managers and serves on a variety of high-level committees, including the technology executive steering committee, the patient safety committee, and the operations planning board.

Vogt was surprised by the amount of HIPAA-related advice she has provided and how broad the audience has been, ranging from executive leaders to managers in areas such as research, marketing, and fundraising. She even talks HIPAA regulation to vendors and other providers in the community. "I get a lot of calls from nursing homes and physician offices that don't have the resources for a full-time privacy officer," says Vogt. During the compliance stage, she averaged 350 e-mails and 100 calls a week; these days the volume is definitely down, but it is still steady. Vogt views that as a positive sign because it shows that people are aware of HIPAA and know who to contact when questions arise.

Vogt even began negotiating the business associate agreements required by HIPAA. Aurora Health Care acts as a business associate for some of its covered entities, and there was no one who routinely negotiated these agreements. To date, Vogt has worked on nearly 60 such agreements.

Pitching in for the Security Rule

Because privacy and security go hand in hand, privacy officers are working with their organizations' security officers to implement the next phase of HIPAA, which ensures the security of health information. The rule goes into effect April 2005 and 2006, depending on the size of the organization. While many privacy officers serve on a security committee or task force and are involved with the security risk assessment, their involvement is usually limited to the privacy aspects of the security rule.

At Tallahassee Memorial, Monello meets weekly with the security officer to address training and implementation. "We're using some of the valuable lessons from implementing the privacy rule to address security in a better way," she says, adding that the most valuable lesson she learned was to have a thorough knowledge and understanding of the rule itself. "Reading it, studying it, and seeing how others are interpreting it give you the ability to move forward more quickly with the rule," says Monello. Consequently, she is encouraging the security officer to have a solid understanding of the rule and to "appoint deputies of knowledge" who are well-versed in various aspects of it.

(For more on how organizations are leveraging their privacy experience as they prepare for the security rule implementation, see "Preparing for the Next Big April" *Journal of AHIMA*, 75:4.)

The Years Ahead

As HIPAA is tested in the legal arena, privacy officers believe that they will receive greater visibility within their organizations. Many anticipate working even more closely with risk managers to address related organizational risk management issues that may result from sanctions or civil suits. As more and more organizations move from paper or hybrid records to electronic health records, the more critical the role privacy officers will play in that transition.

Meanwhile, privacy officers have their hands full. "I've worked in HIM for 26 years, and I thought I'd have to sell privacy when I took on this role. But there was already a strong culture and commitment to it. I'm just trying to keep up with the volume," says Vogt, concluding, "It's very rewarding, because people are so appreciative when they get advice. I feel like I'm collaborating with the whole organization."

Knowledge and Skills for the Privacy Officer

What knowledge and skills does it take to be a privacy officer?

A good understanding of health information management, specifically a strong knowledge of release of information, is crucial. But as Mangin notes, "That's what's so beautiful about the RHIT and RHIA credentials. That's part of the training we receive in our program. We were born to do this job."

Monello, who passed the CHP examination last December, adds that pursuing the privacy credential is also beneficial. "Not only does it test your own knowledge and show you where you need to focus your attention, but it also assures others that you're competent in this area."

Next is the ability to read and interpret federal, state, and any other applicable regulatory laws. Mangin spent a lot of time on AHIMA's HIPAA Community of Practice (CoP) and HIPAA: Privacy Officer CoP, networking with peers and bouncing interpretations off them. "The CoPs have been a wonderful resource," she says. "I used them heavily leading up to last April and continue to use them."

The ability to analyze risks objectively is critical, because privacy officers spend so much time analyzing the risk of conducting a process one way or another, says Vogt. The ability to make reasonable decisions quickly goes hand in hand. "I can't send everything to a committee and wait two months for a response," says Vogt. "A lot of what I do on a daily basis requires an immediate decision."

Monello concurs. "You need to have confidence in your ability to make decisions based on your knowledge, because you are regarded as the HIPAA expert in your organization."

The skill set for privacy officers includes computer skills to comfortably navigate and manipulate databases, project management skills to juggle the multitude of projects that touch on HIPAA, and training skills to engage individuals across the organization and even outside of it.

Good communication skills don't hurt, either. "We're used to communicating with peers inside and outside of the organization," says Monello. "But now we're faced with having to communicate with patients who are often upset because they have complaints about privacy violations."

No "Typical Day" in the Life of a Privacy Officer

Because many privacy officers are not solely devoted to addressing the privacy rule, their jobs require them to juggle HIPAA-related responsibilities with HIM responsibilities. Most days, the two intertwine.

Daily tasks of a privacy officer include:

- Responding to HIPAA-related questions
- Providing training
- Running audit reports
- Addressing requests for release of information
- Investigating patient complaints
- Attending meetings with HIPAA issues on the agenda

As one privacy officer sums up the day's possible duties, "It's very unpredictable as far as what may come your way."

Ruth Carol *(ruthcarol1@aol.com) is a Chicago-based freelance writer specializing in healthcare issues.*

Article citation:
Carol, Ruth. "Busier Than Ever: Privacy Officers One Year Later." *Journal of AHIMA* 75, no.4 (April 2004): 20-23.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.