Taking Pages from Other Notebooks: What Lessons Can Chief Privacy Officers Learn from Other Industries?

Save to myBoK

by Mark Hagland

HIM professionals are stepping up to the newly created role of privacy officer in many organizations. But privacy officers have been around for years in other industries. What can we learn from them about positioning this role?

Banking and financial services, telecommunications, and other industries are already working through regulatory requirements on privacy; healthcare is up next, with HIPAA's chief privacy officer mandate. Many HIM professionals are moving into these new roles, and experts fluent in cross-industry trends are urging healthcare leaders to look to other industries for cues as they move toward the target date for implementation.

With healthcare organizations beginning the scramble to satisfy the federal government's privacy requirements under the privacy rule of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, more and more are starting to consider where and how to find the chief privacy officer (CPO) they will be required to name by April 2003. Relatively few have made an attempt to look at how CPO positions have developed in other service industries from banking and financial services to the airlines and transportation, hotels and hospitality, and retailing, yet there are abundant opportunities to take a page from other notebooks.

No one questions that there are some fundamental differences between healthcare and other service industries. At the same time, all those fields have had experience with implementing privacy regimens, and one, banking and financial services, already has its own HIPAA in the form of the privacy rule in the Graham-Leach-Bliley Act (GLB) of 1999. This law was created to safeguard consumer privacy at the time that federal legislators opened the gates to freer affiliations among different types of financial institutions—banks, brokerage firms, financial services companies, and insurers. Meanwhile, every industry involved with consumers is undergoing change as the demands for data and information privacy grow along with consumers' awareness and empowerment.

Nationwide's Double Jump

Indeed, anyone in healthcare considering how to think about HIPAA and its CPO mandate might want to hear about Kirk Herath's experience. Herath, chief privacy and public policy officer for Nationwide Insurance Companies, Columbus, OH, can speak to privacy demands being made on both the healthcare and financial services sides of his organization. Nationwide, a diversified insurance and financial services company, offers investment and financial services, non-healthcare insurance (auto, life, and homeowners' insurance), and a health plan. And, says Herath, Nationwide's experiences in satisfying both HIPAA and GLB have been rigorous, instructive, and highly comparable.

Herath, who has been with Nationwide for a number of years, was named chief privacy and public policy officer in April 2000. Previously, he had been a lobbyist for the company, and, as he explains it, "I was for many years the issues manager for the whole corporation; I was the guy whose job it was to identify macro issues that will impact us sort of globally but haven't been on everybody's radar screen yet." Herath says he identified privacy as an issue in the mid-1990s and became aware of the issue on the healthcare side of the corporation after the National Association of Insurance Commissioners cited privacy as a major issue for health insurers and providers, months before HIPAA was passed in 1996.

That said, preparation for GLB came first. "We spent almost all of 1999 working on defining what privacy was going to mean in terms of GLB, which passed in November 1999," Herath reports. "I had the task as early as 1997, really, for the corporation to sort of head up an interoffice, cross-functional workgroup. I became chairperson of it and reported to the CEO on privacy and the risks. Having already developed that cross-functional work group, we had developed a draft set of privacy principles in

1997. And we had done some surveys internally in 1998 to see how we matched up to our principles, so we knew where our gaps were."

Herath was appointed CPO just after GLB was passed, and the next phase of development of privacy on the financial services and insurance side of Nationwide was for Herath and his colleagues to "determine which areas owned privacy from an implementation perspective, who was going to drive it, and where the resources were going to come from," he recalls. Fortunately, Herath says, "We had a very proactive chief of information security at the time, who determined that privacy would be a problem, so he literally gave me two of his staff for a year"—a new director of privacy and a privacy consultant. In addition to the two formal privacy officers who worked for him, Herath says he was able to take advantage of the time and efforts of "many dozens" of other Nationwide staffers who do some work for the "virtual privacy office" he and his colleagues have created at the company. As in patient care organizations in healthcare, Herath is able to gather together resources beyond formal staff in his privacy development efforts.

Because of such organization-wide support, Nationwide is quite far along in its development of a full privacy regimen for GLB on the financial services side, with policies and procedures largely in place now. When asked what the biggest challenges have been in terms of the development of a privacy regimen for GLB, Herath says simply, "Getting started. GLB was huge, and HIPAA's even larger . . . You look at this beast, and you can't quite fathom how you're going to play it," he says, immediately linking the lessons of preparing for GLB on the financial services side of his company with those of preparing for HIPAA on the health plan side. In fact, Herath says, they are very similar.

The key lesson he's learned? "You've got to disassemble it," whether it is preparation for GLB or for HIPAA. "You've got to have an organization and a work plan that gets to the end on time." Herath compares working on either GLB or HIPAA to running a political campaign, with its ups and downs and need for flexibility and discipline across a long haul. And, he adds, it is crucial to name a CPO early on and give that person the full and evident support of executive management, especially the CEO.

Even choosing the CPO from the ranks of the organization is a similar process in both industries, he contends. There is no single person in either industry who is "ideally" suited to the task; the choice depends on the nature of the organization, the people in the organization, and the strengths and qualifications of individuals who are in the organization or recruitable to it.

CPOs Emerge Across Industries: A Trend

The challenges of finding CPOs are indeed similar across business fields, say cross-industry experts on CPOs. For example, the banking and financial services area was faced with the mandate to create privacy regimens earlier than the healthcare industry (GLB required banks and financial services organizations to have their privacy plans in place last year). Perhaps one-third or fewer of the 5,000 to 6,000 consumer banks in the US have appointed a CPO to date (although appointing a CPO was not an explicit requirement of GLB as it is in HIPAA). More are doing so every day, however, reports Alan Westin, PhD, JD, president of Privacy & American Business (www.pandab.org), a nonprofit organization launched in 1993 as an activity of the Center for Social & Legal Research, a global think tank exploring consumer and employee data and privacy protection issues. Privacy & American Business' mission is to educate on the subject of privacy and CPOs across industries, including promotion of the development of the CPO position.

"Before 1999," Westin says, "five to 10 percent of the leading companies in financial services and in telecommunications had already designated somebody to be their privacy officer, often an official from government affairs, consumer affairs, or someone from their e-commerce task force." Those individuals, he says, generally tracked privacy issues and worked on proactive privacy policies. But in 1999, he notes, privacy really became highlighted as an issue, and the passage of both HIPAA and GLB accelerated that process in consumer services industries.

What is of particular interest for healthcare leaders, Westin says, is what happened in the financial services world in this privacy regimen area. In banking and financial services, a small group of leading organizations—American Express, CitiGroup, Chase, Bank of America—moved quickly and decisively to develop transparent, consumer-friendly privacy policies, with the idea that this was another area in which they could achieve greater confidence on the part of consumers and thus further their competitive edge. (Banking and financial services organizations, like healthcare organizations, he notes, are working in a heavily regulated industry and are accustomed to an ongoing procession of new regulatory requirements.)

Similarly, in the telecommunications industry, firms had to determine how they would "communicate to consumers the rules about switching their service from their present carrier to other carriers, and about how they marketed to consumers. Those privacy officers who approached the requirement by creating focus groups of consumers of national populations learned how to write messages that were seen by their customers as trustworthy and credible. In contrast, a lot of companies let their lawyers write these policies and messages, and they were absolute disasters."

The lesson in all this? "The privacy officer in healthcare has to be even more a champion of consumers' interests than does the CPO in the financial services and telecom worlds," Westin asserts. "In the financial services world, everyone's competing for banking and credit card customers. In the financial services area, you have not gotten and will not get the same kind of hostility, confrontation, and litigation that I see coming in the healthcare field if healthcare consumers feel they're not treated well."

Time to Move Toward Competitive Business Advantage—And Integrate

Lessons learned from the banking and financial services industry are eminently transferable to healthcare per HIPAA, says Doron Rotman, a partner in the Silicon Valley office of diversified consulting firm KPMG. Because of both GLB and the revised Fair Credit Reporting Act (FCRA) of 1999, says the Mountain View, CA-based Rotman, privacy concerns over financial organizations operating multiple types of businesses have led to an earlier awareness of privacy concerns than in healthcare.

"In banking," Rotman says, "concern over privacy was probably embedded in organizations at a higher level. The FCRA required the privacy of financial information and examination of issues around identity theft and so on in recent years. So it was probably easy to find people with the understanding" of privacy issues. More specifically, he says, the key lesson learned from GLB and the FCRA in banking and financial services was that "If you want to succeed, you need the buy-in of what I'll call the business side. Privacy cannot be an issue only of legal, or of information, security; it should be a business issue."

Rotman and his colleagues at KPMG have authored a white paper on privacy. Its very title demonstrates how the firm feels about privacy management: "A New Covenant with Stakeholders: Managing Privacy as a Competitive Advantage." Rotman says that healthcare organizations can learn the lesson of potential competitive advantage from the experience of banks, financial services companies, and telecommunications companies. "Patients are really concerned about their health information, and if they are faced with two providers with more or less the same coverage, price range, and so on, and one of them has a real commitment to privacy, that commitment should help that provider. People are starting to look at privacy as a differentiator."

Indeed, the Marriottsville, MD-based Bon Secours Health System—a patient care organization that KPMG featured in its report as moving forward on efforts to manage privacy as a competitive advantage in healthcare—is doing just that. Mike Fabrizius, the system's corporate responsibility officer, is in charge of compliance for Bon Secours hospitals.

"Philosophically, we don't think either HIPAA compliance or privacy management should be a stand-alone issue," says Fabrizius. "We think it should be integrated into our overall management." In that context, he says, "We view the HIPAA regulations as part of our privacy responsibility." Fabrizius says he and his colleagues are trying to pursue as integrated an approach to HIPAA as possible. They have not yet named a CPO, although it is clear that Fabrizius himself currently performs that role and will supervise the CPO and his or her staff once that individual is named.

In any case, Fabrizius says, his work on the privacy regimen for Bon Secours so far—careful development of an overall privacy strategy and collaborative, interdepartmental work on a draft privacy proposal that is currently being reviewed, with implementation plans set to move forward this winter and spring—has convinced him that patient care organizations like his need to both work with alacrity to place CPOs in the next year and consider how other industries have done so.

Healthcare CPOs, he says, need to have skill sets comparable to those of CPOs in other industries. These include good leadership and facilitator skills, the ability to mobilize large virtual teams to assess privacy practices and develop new policies as necessary, and the ability to communicate effectively with executive management and the board. In fact, Fabrizius says, the governance level in patient care organizations will become increasingly interested in how the CPO manages privacy policies and procedures over time. And, as in other industries, staff education will be critical to the success of privacy regimens in

healthcare. "A well-educated, well-informed work force," he insists, "will be the best insurance we have in complying with HIPAA's privacy requirements."

Certainly, all those interviewed agree, there is no time to be lost. Indeed, experts and those in the trenches say that privacy leaders in patient care organizations need to gather intelligence from other industries, and from healthcare organizations that have studied other industries, now. And they need to apply those lessons intelligently and expeditiously as they develop CPO positions and privacy regimens.

In the end, Nationwide's Herath says, the key lesson from all the experiences of the different US business fields on privacy "is uniformity across an organization. You've got to get out of your parochial silos. The cross-functional team is so powerful. With a well-functioning, cross-functional team, whatever you build is better." Given the short span of time at our industry's disposal, he adds, no healthcare organization—hospital, health system, medical group, or health insurer—can afford to wait on privacy officer and privacy regimen preparation. The time is now, he emphasizes, and the lessons are everywhere to be gathered.

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

Key Lessons Learned from other Industries

The experiences of other industries in complying with federal regulatory innovations on consumer privacy, and in managing the public's increasingly sophisticated expectations on privacy protections, are many. Those cited by cross-industry experts that can be applied to healthcare organizations' development of the chief privacy officer (CPO) position, support for that position, and development of privacy regimens, include the following:

- In all industries, developing an organization's privacy strategy and naming a CPO and the CPO's staff is a time-intensive and interdepartmental endeavor. **Don't underestimate** the time, effort, and expense involved.
- CPOs can come from a variety of backgrounds within an organization or as individuals who bring diverse qualifications from outside. But the hunt for individuals with **leadership, organizational, and team-building skills**, along with appropriate general technical understanding of the privacy issues at hand, is universal across industries.
- In the banking, financial services, and telecommunications industries, organizations that have made communicating about privacy a **top strategic priority** and seen regulatory consumer privacy mandates as **opportunities for differentiation** have gained competitive market advantage.
- Conversely, in those industries, "follower" organizations that have approached privacy mandates as **necessary evils and minimized their strategic implications** have reaped public and media scrutiny and criticism.
- Across different industries, CPOs have come to rely on two key elements for success. **Rock-solid support** from executive management and governance levels and **resources and participation** of individuals from many departments and divisions within their organizations are critical.
- The concept of the CPO position is still evolving, even in the banking and financial services industries. But all industries can look to pioneering organizations that have formulated the CPO position and developed privacy regimens for **strategic cues**.

Learn More Online

- To access the KPMG white paper on privacy, "A New Covenant with Stakeholders: Managing Privacy as a Competitive Advantage," go to http://www.kpmg.com/ Rut2000_prod/Documents/9/Privacy_web.pdf.
- To learn more about the Privacy & American Business organization, go to www.pandab.org.

Article citation:
Hagland, Mark. "Taking Pages From Other Notebooks: What Lessons Can Chief Privacy Officers Learn From Other Industries?" *Journal of AHIMA* 73, no.2 (2002): 20-24.

Driving the Power of Knowledge

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