The New Privacy Officer

Save to myBoK

By Chris Dimick

It has been a decade since the first privacy officers took their jobs in response to the HIPAA privacy rule. A slew of changes since then have added more responsibility, required more skills, and demanded more time of them than anyone could have imagined.

When Nancy Davis, RHIA, was first appointed as a privacy officer in 2002, the position was intended to last one year. Set up HIPAA-compliant processes, train staff on the new regulation, and then occasionally refresh the program. Done.

Ten years later Davis is still the director of privacy and the security officer at Ministry Health Care in Wisconsin, and her program still isn't "done." In fact, she has few routine, work-a-day duties-her role continues to evolve.

"I've been doing this for 10 years, and I don't feel like I'm doing 'maintenance' work yet," she says. "There always seems to be something happening."

The privacy officer role has changed immensely since it was first mandated for covered entities under HIPAA in 2003. Privacy officers have seen their jobs grow as new regulations, technology, and data-sharing initiatives have reshaped the landscape. Protecting patient health information has become much more complex since 2003, when nearly all healthcare organizations used time-tested systems to protect paper records.

In turn privacy officers now require an expanding set of knowledge and skills, and as regulatory pressures and technological initiatives have advanced, their roles have grown in strategic importance within their organizations.

Regulation Changes Roles

One of the biggest changes to the privacy officer role came with the passage of the HITECH Act in 2009. HITECH, a part of the broader American Recovery and Reinvestment Act, introduced the biggest set of changes in health information privacy regulation since HIPAA.

HITECH provisions modified and added to HIPAA, sending healthcare facilities and their privacy officers scrambling to understand and respond to stricter privacy protections, better information access tracking, and steeper penalties for noncompliance.

Responding to the Breach Notification Rule

The HITECH provision that has had the biggest impact to date is the breach notification rule. The interim rule, which is still awaiting its final version, requires healthcare facilities and their business associates to investigate and provide notification following a breach of unsecured protected health information.

The rule describes how covered entities must notify individuals and the Department of Health and Human Services. In breaches affecting 500 or more individuals, covered entities must notify HHS and local media without unreasonable delay and within 60 days of discovery.

Privacy officers quickly saw their role heightened in awareness and importance.

A corporate privacy officer for 10 years at multifacility hospital system Orlando Health, Linda Noel, MEd, RHIA, has seen her role drastically change over the last several years due to HITECH's breach notification rule.

"While the early years were focused on implementation, policy writing, and education, my role has now changed to investigator," Noel says. "Most of my time is spent completing risk assessments and documenting [privacy incident] cases."

When a privacy breach is suspected, privacy officers now must drop everything and begin their investigation in order to determine if a breach occurred and, if so, how to mitigate the damages and determine who is responsible.

A challenging aspect of the rule has been the so-called harm threshold, which allows organizations to forego notification if they determine that a breach is unlikely to pose harm to the individuals. Lacking direct guidance in the rule, privacy officers and their colleagues had to establish protocols and parameters for assessing and documenting potential for harm.

The in-depth investigations required the acquisition of new skills. They also required a reorganization of job duties, as breaches have been taking up large amounts of a privacy officer's time, says Angela Dinh, MHA, RHIA, CHPS, professional practice director at AHIMA.

For privacy officers overseeing several facilities, workload has skyrocketed. Davis's workload doubled, she says, as she worked with local organization privacy officers to help determine the risk of harm in individual privacy incidents.

Under the Compliance Umbrella

When privacy and security officer jobs were first created, they typically were placed in HIM departments. Recently some facilities have moved the role to their compliance departments. The move is mainly strategic. As HIPAA enforcement ramps up, some organizations consider that privacy has become closer in function to compliance.

"Privacy has truly become sort of its own world, an offshoot of HIM and IT," Davis says. "It has become its own operational function, and it just seems logical to have it connected to compliance."

The privacy and security officer role at St. Charles Health System was purposefully designed within the compliance department, not HIM, says Hofman, the system's privacy and information security officer. While she feels her HIM expertise is invaluable to her role, aligning the role with compliance positions her to not just monitor medical records but also have oversight of the entire system's operations and compliance efforts, she says. Over the years Hofman has taken on more compliance-related duties as the privacy and security officer.

"This gives us an opportunity to have an oversight on the release of records and audit without feeling like there is a conflict of interest with medical records," she says.

More Rulemaking to Come

Two of the biggest modifications to HIPAA have yet to take effect. In fact, they have yet to receive final rules.

HITECH expanded a patient's rights to an accounting of the disclosures of their health information. Given the burden associated with accounting for disclosures-and the faint interest patients have shown in receiving them-the announcement put covered entities on edge waiting for the actual rulemaking.

In its proposed rule the Office for Civil Rights sought to shift the focus from disclosures to access, proposing that covered entities create and maintain access reports that would show patients, upon request, who had accessed their information kept in electronic health records.

Though the industry generally supported the attempt to ease the accounting of disclosures burden, many still saw significant challenges in producing access reports. OCR is handling the accounting of disclosure provision in rulemaking separate from the other HITECH privacy-related measures. A final rule is expected this year, and when it arrives privacy officers are expecting a busy time teasing apart the rule and helping bring their organizations into compliance.

Another HITECH provision enables patients who pay for treatment out of pocket to request that the information regarding the encounter not be reported to insurance companies. Covered entities would be required to comply.

HIM professionals and privacy officers are still figuring out how they would sequester information for these types of requests using today's EHR systems. They will also require processes to ensure that months down the line the information is not inadvertently disclosed in a routine record request.

HITECH's modifications to the privacy rule have caused many privacy officers to develop their research skills and legal knowledge. These are necessary in order to dig into statutes, interpret the law, and then apply it back to their own facility.

Regulatory knowledge and having the ability to track state and federal changes have always been key privacy officer skills, but never more so than now, Dinh says.

"Today's privacy officer really has to stay on top of the always-changing regulations and industry practices," she says. In fact, even that may not be enough-"It's almost like they have to be one step ahead."

OCR Gets Serious about Enforcement

HITECH also strengthened the civil and criminal enforcement of HIPAA.

The enforcement rule raised the maximum penalty amount for a HIPAA violation to $1.5 million, and also spurred HHS and OCR to step up their enforcement of HIPAA through privacy and security audits and investigations.

The pressure increased on privacy officers and their organizations to perform regular audits, fully document privacy violation investigations, and update policies on completing risk assessments.

In turn privacy officers needed to sharpen their investigative skills, their ability to organize and work with databases, and respond to government audits like those performed by OCR, says Judi Hofman, CAP, CHP, CHSS, the privacy and information security officer at St. Charles Health System in Bend, OR.

Once an idle threat, OCR has followed through on HITECH's promise to investigate privacy and security breaches. Hofman has led her organization through two OCR audits, requiring her to increase her knowledge of federal regulations and the auditing process.

As OCR and HHS continue to promote patient privacy rights to the public, government investigations will only increase as violation reports go up, requiring all privacy officers to adapt their skills in order to be prepared for an investigation.

Technology Changes Roles

In the years since HIPAA mandated the privacy officer role, health IT has radically changed the way privacy officers work. Technology has made the role more complex, Dinh says, because privacy officers must have a good understanding of electronic systems.

They must keep current on emerging technologies and the impact they could have on patient privacy. They must be able to make recommendations on technology and technology-driven data sharing such as health information exchange networks.

The increase in the adoption of EHR systems since 2003 has caused privacy officers to look at their protection policies and procedures and adapt them for the new environment.

"I think the role has continued to change, has continued to be challenging, partially because the laws have changed, but also partially because the environment has changed," Davis says.

Hofman's job changed drastically both times St. Charles implemented an EHR, she says. She worked with departments including human resources to define the appropriate data access permissions, sorting out which staff had access to patient records and determining the correct level of access.

Discovering and mitigating the unique privacy risks that EHRs pose required privacy officers to add technology expertise in short order.

Further, EHRs changed the way privacy officers could monitor who accessed patient records. Hofman had to learn how to use the EHR and other ancillary systems to audit records and assess processes.

An EHR offers a broader tool for monitoring privacy compliance, she notes, but it also means "there is a lot more to look at."

Even voluntary federal programs are having an impact on privacy officers. Patient engagement objectives in the meaningful use EHR incentive program require participants furnish patients with electronic copies of their medical records upon request. Privacy officers must work with colleagues to devise policies and procedures for protecting patient information when it is copied to a CD or delivered through a Web portal.

The development of risk management skills and even quality improvement skills are now necessary for privacy officers as they search for ways to mitigate risk in the EHR and other processes, Davis says.

Social Media and Mobile Devices

As the record becomes more accessible, it must also become more secure.

Health IT and EHRs allow easier manipulation and sharing of data. Privacy officers have recently found themselves in the position of the data usage police, calling into question necessary privacy and security questions when organizations look for new ways of using their health information-be it for population health research, marketing, or new care processes.

Doctors in a facility may want to use mobile devices to text each other PHI, but it's up to a privacy officer to call into question the vulnerabilities of such uses. As social media has become more prevalent, it's become necessary for privacy officers to understand and be able to investigate privacy concerns that can arise in those environments. These social media skills are all new to the position.

"Over the years we were always promised the technology would be there, and we waited and waited," Davis says. "Now it is there and we can do anything. But the important thing is somebody has got to be asking the 'should' question."

Health Information Exchanges Change Roles

When facilities began planning the exchange of health records with other organizations through health information exchange networks, privacy officers took note, Davis says. HIEs offer benefits to patient care, but ensuring appropriate privacy protections have made the privacy officer's job more complicated and more vital.

Privacy and security is one of the biggest issues in health information exchange, Dinh says. With so much electronic PHI in transit from multiple sources, facilities must ensure the right information is going to the right recipient.

While privacy officers have been monitoring the exchange of information since their early days in 2003, it was mostly limited to paper mail and fax. Now they must employ different techniques to protect patient information during transit.

As HIEs grow, privacy officers are devoting more time to drawing up HIE policies and collaborating on electronic methods to protect information, such as encryption and content permissions.

Data integrity is an added concern. Even when the correct patient data arrive securely at the correct destination it must arrive unaltered and be correctly interpreted, Dinh notes.

HIE has changed the patient consent process. Privacy officers have had to help develop policies and practices for obtaining patient consent before exchanges take place. Consent for participation in an HIE is much more complex and far reaching, requiring modified and more technical consent authorizations.

At Ministry Health, Davis took part in negotiations with an information exchange partner regarding what privacy policies would be followed and whether or not exchanged information would become part of the legal health record. These privacy

negotiation skills are a new requirement for privacy officers working in facilities that take part in local or state-wide HIEs.

"You have to really work collaboratively in order to come up with exchange policies that everyone can live with," Davis says.

When the security officer position was mandated by a HIPAA update in 2005, many privacy officers absorbed the security role. This led to an entirely new technical skill set that needed to be learned, Hofman says. The implementation of health IT systems helped meld the line between privacy officer and security officer skills, Hofman says.

"It is a very gray line between privacy and information security now," she says.

While privacy and security officers do not get involved in the actual technical implementation-that is done by IT departments-they do need to know enough to ensure a product will protect a facility as well as allow proper access. This takes project management and technical skills, two job requirements that have been added to privacy and security officers' job role over the last few years.

"As privacy officers may take over HIPAA security functions as well, certainly your skill set is going to have to change and you are going to have to be technically savvy about systems, firewalls, [and] security applications out there on the market," Hofman says. "It does make a very complex position when you are oversight for both."

Chief Privacy Officers Emerging

With increased visibility, privacy officers now are in charge of more responsibilities and projects than they were in 2003. Over the years that Chrisann Lemery, RHIA, FAHIMA, has handled privacy matters as the compliance specialist at WEA Trust Insurance she has become recognized as the individual who understands both the privacy issues and the processes for moving health data internally and externally.

Because of this, the health plan has used Lemery's privacy investigations as a springboard to perform and coordinate business process re-engineering in order to prevent risks of disclosing or using data inappropriately.

While her first duties focused on documenting and implementing privacy policies and procedures, today Lemery's role has moved to more analysis and refinement of those procedures in order to prevent mishaps, she says.

Healthcare leaders have recognized how important proper privacy and security processes are to an organization and how many areas these processes touch. In response, some health systems have created a chief privacy officer role.

This elevation to the C-suite enables chief privacy officers to infuse and monitor privacy and security practices throughout an organization, as well as manage privacy officers at satellite facilities to ensure state and federal regulations are implemented and practiced uniformly, Dinh says.

Multirole Privacy Officers Squeezed

When the privacy officer role was first created, many organizations bundled it into the HIM director's responsibilities. At the time it seemed like a manageable request, and many HIM directors/privacy officers took on the role as "other duties assigned," Davis says.

But as the responsibilities and workload increased over the years, the privacy duties have required more and more time of otherwise busy HIM directors. Splitting off the role into its own position, however, is not always possible, especially at smaller facilities.

Combining too many roles-HIM director/privacy officer/security officer/compliance officer, for instance-can cause erosion in each of those disciplines, Hofman notes.

"You are not going to have a lot of time to focus on your privacy initiatives if you are a medical records director running coding with ICD-10," she says. "Organizations need to be careful as they try to streamline positions."

In California, privacy officers were adapting to a stringent new state law on breach notification in the months before HITECH was passed. The California law mandates breach reporting within five days of discovery, the strictest requirement in the country.

Daniel Pothen, MS, RHIA, CHPS, CCS-P, serves as the director of clinical informatics/HIS/privacy officer at Mission Hospital based in Mission Viejo, CA. He has seen the privacy officer portion of his job increase in importance in the years since the state and federal breach laws were passed.

California's breach law required Pothen to rework the organization's breach policies and educate staff on the new requirements. When the federal breach notification law took effect later that year, Pothen and other privacy officers statewide had to assess its requirements against their state law to ensure their organizational practices would keep them compliant with both regulations.

Breach investigations continue to eat up time for multirole privacy officers like Pothen. California's five-day notification deadline adds urgency to the effort.

"It is very time intensive when you have to basically stop what you are doing, drop everything, and investigate a suspected privacy breach," Pothen says.

Pothen has turned to his compliance coordinator for help when breaches occur, which allows him to meet the five-day notification law while also handling his other duties as director of clinical informatics and health information services. Strong management support has also helped him fulfill his various responsibilities-something that is essential today for all multi-role privacy officers.

As privacy officers become busier, they need to develop their skills in collaborating with other staff members to share and leverage work, Hofman says.

They need to assess what they are doing internally and then seek out potential partners who are addressing the same issues.

As more duties are handed to the privacy officer over the coming years, Dinh foresees the role becoming a full-time position at most facilities.

"There is a good possibility that the privacy officer's responsibilities are going to become so big that being the HIM director/privacy officer won't be an option. It will become a position of its own," she says.

At its core, the privacy officer's duty remains unchanged; however, the role has changed greatly since it was conceived as a temporary or part-time position back in 2002, Davis says.

"I think when we went into this 10 years ago we didn't know what we would be doing and how long we would be doing it for," she explains. "There is much greater definition of the role now, there is greater responsibility, and great recognition."

Chris Dimick (chris.dimick@ahima.org) is staff writer at the *Journal of AHIMA*.

Article citation:
Dimick, Chris. "The New Privacy Officer" *Journal of AHIMA* 83, no.4 (April 2012): 20-25.