Seven Select Questions to Ask Your Privacy Officer (Or Yourself)

By Katherine Downing, MA, RHIA, CHPS, PMP

On January 25, 2013, the US Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) published the long-awaited HITECH-HIPAA Omnibus Final Rule in the *Federal Register*. As anticipated, the Omnibus Rule includes some of the most significant changes to patient privacy since HIPAA was first fully enacted in 2003. Covered entities needed to be in compliance with the Omnibus Rule by September 23, 2013.

While the rule changes have caused some headaches, the good news is that the Omnibus Rule gives health information management (HIM) professionals the opportunity to expand upon their already well-honed abilities to ensure the privacy and protection of patient health information. HIM professionals have always advocated for patient privacy within their healthcare organizations by insisting upon professional accountability and the implementation of patient protection directives. Protecting patient privacy requires a delicate balance between restricting information to ensure confidentiality while also giving providers and others access to that information for patient care and payment.

Many HIM professionals now serve in the role of chief privacy officer, providing leadership and ensuring compliance with HIPAA and other rules. Whether you are the privacy and security officer, or this role is held by others, the following are some key questions to ask as the healthcare industry advances through 2014.

1. Are we confident in our workforce education program for privacy and security?

The definition of workforce was updated in HITECH to mean "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a [HIPAA-] covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate."

All workforce members who use and access protected health information (PHI), including current and new employees, must be trained on an organization's privacy policies. Staff members must receive retraining when changes occur to an organization's rules, policies, or procedures. An example is the HITECH-HIPAA Omnibus Rule's new requirements for the right to request restrictions. The HITECH Act extends some HIPAA privacy and security provisions, and it also adds new regulations that affect all workforce members. Thus organizations must ensure that members of their workforce are aware of these rules and their application as well as any relevant policies and procedures. Covered entities should work closely with business associates to ensure that privacy and security training occurs in accordance with HIPAA requirements.[1]

2. What are the breach notification policies and procedures?

The HIPAA Breach Notification Rule requires healthcare providers, health plans, and other HIPAA-covered entities to notify affected individuals and OCR when health information is breached. In addition to the reporting requirements for all breaches, breaches that affect more than 500 individuals must be reported to the HHS Secretary and the media. Under HITECH, the HHS Secretary is required to post a list of these breaches on the department's website, which is available at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html. The timelines for reporting breaches are different for breaches under and over 500 individuals within a state. This should be taken into account when building one's local program.

As a result of these regulations, media reports of healthcare privacy and security breaches continue to increase in number and scope. These reports threaten efforts to build consumer trust in electronic health records (EHR), health information exchange

(HIE), and healthcare reform. Healthcare organizations should have a program and policy for breach notification per this rule.

In a perfect world, access controls alone would ensure the privacy and security of electronic PHI (ePHI). However, the complexities of today's healthcare environment make it extremely challenging to limit access to the minimum necessary information that members of the workforce require to perform their jobs. HIPAA audits can be a product of routine proactive auditing or based on a patient complaint, so policies for both situations should be in place to minimize the risk of a possible breach.[2]

3. Are mobile devices and laptops that store, transmit, and access PHI secured with encryption?

Technology has great power to improve healthcare. But with that great power comes great responsibility, according to Joy Pritts, chief privacy officer at HHS' Office of the National Coordinator for Health Information Technology (ONC). "The use of mobile health technology holds great promise in improving health and health care, but the loss of health information can have a devastating impact on the trust that patients have in their providers. It's important that these tools are used correctly," Pritts said in a statement. "Health care providers, administrators and their staffs must create a culture of privacy and security across their organizations to ensure the privacy and security of their patients' protected health information."

Investing in the protection of mobile devices is one of the industry's greatest challenges. A 2012 study by the Ponemon Institute revealed that 94 percent of healthcare organizations have suffered at least one data breach, while an astounding 45 percent of organizations have experienced more than five data breaches during the past two years.[3]

Encryption is the key to protecting PHI on mobile devices. If a mobile device containing PHI, like a laptop, is lost or stolen but is encrypted, the incident is not considered a privacy breach since the information is encrypted and likely inaccessible. But many healthcare providers have been reluctant to implement encryption due to cost.

4. Is the sanctions policy for HIPAA being applied as written?

The stakes are raised under HITECH-HIPAA enforcement and the potential for harm to an organization has increased greatly. Organizations must ensure that workforce sanctions related to HIPAA privacy and security violations are relevant not only to the incident but also to the potential for compromise of the PHI that was breached. Healthcare organizations should categorize sanctions according to the nature of the privacy or security incident. Categorization helps standardize corrective action determinations, assists with trending privacy and security violations, and makes reporting easier. Two models are outlined in the *Journal of AHIMA's* October 2013 issue Practice Brief titled "Sanction Guidelines for Privacy and Security Violations."[4]

5. Has our organization updated our business associate agreements?

On January 25, 2013, HHS published the final Omnibus Rule which expanded the provisions of HIPAA brought forth in HITECH. The sections affected by these changes include privacy, security, enforcement, and breach notification.

The final Omnibus Rule expanded the definition of a business associate to include subcontractors that create, receive, maintain, or transmit PHI on behalf of another business associate.[5] The definition of the term business associate was also expanded to include:

- Health information organizations
- E-prescribing gateways
- A person that provides data transmission services for PHI exchange on behalf of a covered entity and requires access to such information on a routine basis
- Personal health record (PHR) vendors

In order to be compliant, covered entities and their business associates should review their business associate agreements with the new requirements imposed by the Omnibus Rule. The rule now allows business associates to disclose PHI to their

subcontractors when they enter into a business associate agreement with them. The business associates are responsible and liable to the covered entity for the activities of their subcontractors that have entered into a business associate agreement. If a business associate's contractor becomes aware of a violation of its contractual business associate agreement, it must take steps to cure the breach or terminate the agreement if resolution is unsuccessful.[6]

6. How current is the risk analysis documentation as required by the Security Rule?

Risk analysis is the formal process of examining potential threats and vulnerabilities discovered during the risk assessment and prioritizing those risks based on the probability and potential effect of those risks to the organization and patient. Risks may be mitigated, transferred, or accepted, depending on what option is most reasonable for the organization. Risk analysis is an ongoing process. Any time new health information technology is purchased or when changes to the security rule are implemented, the risk analysis should be repeated.

The HIPAA Security Rule requires covered entities and business associates, as well as their agents and subcontractors, to conduct a risk analysis and implement measures "to sufficiently reduce those risks and vulnerabilities to a reasonable and appropriate level."[7]

The Security Rule applies to a variety of organizations ranging from large healthcare systems to small physician practices as well as their business associates. Thus the standards for how an organization must approach a risk analysis are flexible. An organization must base its decision on several factors, including:

- The organization's size, complexity, and capabilities
- The organization's technical infrastructure, hardware, and software security capabilities
- The costs of security measures
- The probability and criticality of potential risks to ePHI

7. Is the new right to request restrictions policy fully implemented?

The Omnibus Rule, effective September 23, 2013, requires that "a covered entity must agree to the request of an individual to restrict disclosure of protected health information about the individual to a health plan if the disclosure is for the purposes of carrying out payment or health care operations and not otherwise required by law; and the protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full."

This enhancement to the HIPAA Privacy Rule also requires that a statement be included in an organization's Notice of Privacy Practices summarizing the individual's right to a restriction and the covered entity's requirement to accept the restriction to disclose PHI about the individual to a health plan. The rule does not suggest or require how this restriction is to be implemented, only that the covered entity must have a method to note that the information has been restricted and is not released to the health plan for payment or healthcare operations, such as audits.

Each covered entity should have in place a policy and procedure to accept, process, and honor this new rule requirement. See the Practice Brief, "Managing a Patient's Right to Request Restrictions of Disclosures to Health Plans," for more information.

Notes

1. AHIMA. "Privacy and Security Training (Updated)." *Journal of AHIMA* 84, no. 10 (October 2013).
2. AHIMA. "Performing a Breach Risk Assessment." *Journal of AHIMA* 84, no. 9 (Sept 2013): 66-70.
3. Ponemon Institute Library. "Ponemon Study Shows the Cost of a Data Breach Continues to Increase."
4. AHIMA. "Sanction Guidelines for Privacy and Security Violations." *Journal of AHIMA* 84, no. 10 (October 2013).
5. Department of Health and Human Services' Office for Civil Rights. "Business Associate Contracts." January 25, 2013.
6. AHIMA. "Guidelines for a Compliant Business Associate Agreement." November 2013.
7. US Department of Health and Human Services. "The Security Rule."

Katherine Downing (kathy.downing@ahima.org) is a director of HIM practice excellence at AHIMA.

Article citation:
Downing, Katherine. "Seven Select Questions to Ask Your Privacy Officer (Or Yourself)" *Journal of AHIMA* 85, no.4 (April 2014): 42-44.