IGPHC Provides Guidance for Privacy Risk Assessment

Save to myBoK

By Sharon Lewis, MBA, RHIA, CHPS, CPHQ, FAHIMA

In June I delivered a presentation, "Breach Prevention Part I: Take a PHI Pause—Conduct an Actionable Privacy Risk Assessment," at a breakout session at the 2015 California Health Information Convention and Exhibit. Finding resources to create a presentation on conducting an actionable privacy risk assessment was not an easy task. I browsed the AHIMA Body of Knowledge for Practice Briefs and articles, searched the Internet for tools to conduct privacy rounds, and checked the Healthit.gov website. All of this searching led to the same conclusion—there was no tool available to conduct a privacy risk assessment. The National Institute of Standards and Technology (NIST), the Office of the National Coordinator (ONC), and even the California Office of Health Information Integrity (CalOHII) have free tools for conducting a security risk assessment; however, I could not find any type of tool for privacy.

While contemplating my presentation, I was reading AHIMA's Information Governance Principles for Healthcare (IGPHC^{TM}).It dawned on me that one of healthcare's greatest information assets is protected health information (PHI), and to create a culture of compliance we must treat PHI as a valued asset. We must create policies and procedures that are in compliance with all Federal and State Laws and ensure that these policies are being followed, and that employees are trained and committed to the appropriate handling of PHI. Our customer, ultimately, is the patient we treat. As noted by AHIMA in the IGPHC:

> "Trust plays a critical role in healthcare delivery. Patients entrust their personal information to healthcare organizations, creating distinct requirements for confidentiality, privacy and security. These organizations, regardless of their roles in healthcare delivery must earn the confidence of patients and society through a firm commitment to ethical and responsible handling of personal information."

Think about it! Patients must be able to trust that their personal information is confidential, private, and secure and that all healthcare providers, regardless of who or what role they play within the organization are committed to ensuring patients can trust that their information is held in the highest regard.

I began to think about some of the interview questions that should be asked when conducting a privacy round/walkthrough and saw how some could easily be grouped into at least one of the eight principles of information governance. Data could be aggregated and reported. It was a great start to formulating a plan to evaluate what we do with PHI within our organization. As I thought about the process of establishing an information governance program, the thought occurred to me—why not start with the healthcare organization's greatest asset: PHI. The light bulb was on!

To establish a sound program, I needed a framework. The IGPHC was the perfect place to start. The eight principles, Accountability, Transparency, Integrity, Protection, Compliance, Availability, Retention, and Disposition, started my outline. The presentation flowed easily using these principles to guide me.

Accountability establishes the form and format the program will take and requires buy-in from leadership. An information governance committee can be formed to involve stakeholders from various areas to evaluate ongoing compliance.

Transparency ensures that everyone understands their roles and responsibilities and provides for clear communication between all stakeholders. It breaks down silos between privacy, security, compliance, and other departments. As part of policies and procedures, the scope can be defined. All uses and disclosures can be evaluated. Definitions can be clearly established and a documented inventory of where all PHI resides can be completed.

Integrity is directly related to the ability to prove that information is authentic, accurate, timely, and complete. PHI can be evaluated by who (care providers, business associates, legal/regulatory) and how (e-mail, faxing, cloud storage, text/secure messaging) it is used. It means thoroughly defining your legal health record.

Protection ensures that privacy rounds are conducted to determine how well the information is protected from breach, corruption, and loss by monitoring people and process. It evaluates that incident response plans are in place and safeguards are established to limit incidental disclosures of PHI.

Compliance with applicable laws and regulations can be monitored (i.e., Clinical Laboratory Improvement Amendments (CLIA), eDiscovery, Freedom of Information Act, HIPAA, SAMHSA, and FERPA). I thought of compliance as a "retrospective" review, ensuring policies and procedures are in place. Conducting a Privacy and Breach Risk Analysis would assess the risks to privacy by evaluating how well policies and procedures are adhered to and would be the "concurrent" review. There are a variety of potential threats and vulnerabilities related to privacy that can be assessed.

Availability is making sure that the right information is available at the right time. Back-up procedures can be assessed and evaluated. What about downtime processes?

Retention could be tied to minimum use as well as fiscal, operational, clinical, and historical uses of PHI.

And lastly, **Disposition** ensures the information is appropriately discarded in accordance with HIPAA.

By conducting privacy rounds, program measures could easily be established. I created a sample matrix categorized by the principles designed to share with the information governance committee. Communication is a key step toward breach prevention as it keeps awareness high and reminds leaders to keep HIPAA privacy and security in the forefront of leaders' minds.

As HIM professionals, I challenge you to educate yourselves on the principles and initiatives that AHIMA is putting forward regarding IG. It's based on our skillset and understanding regarding how patient information flows (the lifecycle of the record), compliance, and ensuring the information is timely, accurate, available, and confidential. We owe it to the patients we serve. The framework is a path to get us started. The energy and enthusiasm stems from the reason we entered the field in the first place. With the framework of IG as our roadmap, and the strong skillsets of HIM professionals, we can get started. I did!

Acknowledgment

AHIMA thanks ARMA International for use of the following in adapting and creating materials for healthcare industry use in IG adoption: Generally Accepted Recordkeeping Principles® and the Information Governance Maturity Model. ARMA International 2013.

References

AHIMA. "Information Governance Principles for Healthcare (IGPHC)TM." 2014.

Sharon Lewis (slewis@primeauconsultinggroup.com) is principal at Primeau Consulting Group.

Original source:
Lewis, Sharon. "IGPHC Provides Guidance for Privacy Risk Assessment" (Journal of AHIMA website), September 2015.