DIY Privacy Risk Assessments

Save to myBoK

By Mary Butler

The HIM Problem

Completing regular privacy risk assessments is one of the most proactive ways of preventing healthcare privacy breaches. However, finding helpful tools for these assessments is hard to come by.

The HIM Problem Solver: Sharon Lewis, MBA, RHIA, CHPS, CPHQ, FAHIMA, Principal, Primeau Consulting Group

In a blog post written for the *Journal* website's information governance (IG) blog "IGIQ," Sharon Lewis, MBA, RHIA, CHPS, CPHQ, FAHIMA, discussed how she used AHIMA's Information Governance Principles for Healthcare (IGPHC™) to create guidelines to develop a privacy risk assessment. The process Lewis developed through examining the IGPHC is instructive, but it's important to review why risk assessments are so critical in today's security environment.

A privacy risk assessment is not required by HIPAA. Rather, a privacy risk assessment is a best practice to ensure that an organization isn't at risk for a breach. Lewis recently discussed with the *Journal* some tips for devising a framework for a risk assessment and to provide a reminder about why they're needed.

***Journal*: Why did you look to IGPHC for guidance in building a risk analysis framework?**

Lewis: For the HIPAA Security Rule there's all these resources, such as the National Institute of Standards and Technology (NIST) and the Office of the National Coordinator (ONC) that have free tools for conducting a security risk assessment, that provide guidance on how to complete a security risk analysis. On the privacy side there's no help with that. To go through the privacy standards and try to identify what your risks are, it's really difficult.

I tried to think about, what can I create and give to our audience that would be a tangible, actionable approach to doing a privacy risk assessment? So I started looking for things and couldn't come up with anything. I started thinking about the IG principles [IGPHC].

What kind of information and policies should a risk assessment scrutinize?

It's actually around any kind of risk of PHI. So it could be electronic, could be paper, oral, anything that covers aspects of the Privacy Rule, which is safeguarding the verbal, paper, electronic information as it relates to PHI. As I started to dig into it, the privacy rule is very specific to uses and disclosures, so that was my start in identifying where my risks are.

The other thing, as part of this, you really need to define where all of your PHI is, what is used by business associates—what is created, received, maintained, or transmitted. Any place you have PHI or electronic PHI, you want to take an inventory, not only because of the Security Rule, but with privacy, there might be some risks in there that you really want to mitigate. It's important for this group to create an inventory because it can be used across the board for not only security but also privacy.

Why is a risk assessment so important? Is it to prevent breaches and theft of PHI?

If you look at the types of breaches that have occurred, or the breaches by source, a big one I would say is breach prevention, but it's really more mitigation—trying to figure out not IF a breach will occur but WHEN. Trying to mitigate all the potential areas and really catch those areas that are the low-hanging fruit and tackle those. Organizations aren't even really looking at that.

How can organizations get started with risk assessments?

There are different ways they could do it. The way I had proposed was to start by establishing a governance framework and that might be bringing key stakeholders to the table, privacy officer, security officer, HIM, clinical departments, business office, bringing people together to talk about what your potential risks are. So if you establish accountability, one of the first IG principles, and bring those groups together to identify gaps in compliance, you can start taking a look at that and breaking down the silos. That's the first step. Bringing the group together.

And then the next step would be defining your scope, as this group looks at PHI and how are they using the information, disclosing the information, looking at things like role-based access in the health record. It's creating that awareness of what the Privacy Rule defines in what is able to be used or disclosed, and really starting to define what those uses and disclosures are. That starts a whole process.

Who should be taking the lead, when it comes to risk assessments, in healthcare organizations?

This is where I think the chief information governance officer could come into play. I think HIM professionals are the perfect fit for that. I really believe that. I was so excited about using the IGPHC as a framework. As IG came into play, it just made sense. Why not start with PHI as a data element and form a structure around that and bring everything else in?

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.

Mary Butler is the associate editor at The Journal of AHIMA.

Original source:
Butler, Mary. "DIY Privacy Risk Assessments" (Journal of AHIMA website), November 2015.
