COSMOS
Navigate the Compliance Universe

Health Care Privacy Compliance Handbook, 3rd Edition
9. Effective Privacy Risk Assessments

By Dwight Claustre, CHC-F, CHRC, CHPC[1]

As privacy professionals, we want to make sure we have all the tools we need to perform our duties. One of the most important tools is the risk assessment process. The U.S. Department of Health & Human Services (HHS) Office of Inspector General (OIG), the U.S. Federal Sentencing Guidelines, and the HHS Office for Civil Rights (OCR) all stress the importance of conducting risk assessments. In addition, because we all have limited resources, we need a process that will allow us to prioritize the risks. We need a method that offers a way to create our privacy work plan and our privacy audit and monitoring plan.

Ever since the enactment of the Health Insurance Portability and Accountability Act (HIPAA), healthcare providers have been required to conduct risk assessments to help ensure that sensitive health information remains private.

What is a Risk Assessment?

To understand the risk assessment process, let's begin by defining some key terms. "Risk" means the probability or threat of damage, injury, liability, loss, or other negative outcomes. Such outcomes most often will stem from external or internal threats and vulnerabilities.

More broadly, an organization's key risks surround its "organizational assets," which represent any resource or set of resources that the organization values. These would include high-impact programs, physical plants, mission-critical information systems, personnel, equipment, or a logically related group of systems.

When looking to assess risks, an organization must consider possible "threats"—persons or things likely to cause damage or danger to an asset, or any circumstance or event that could adversely affect organizational operations. Additionally, it must be aware of "vulnerabilities"—an asset's inability to withstand the effects of a hostile environment.

Putting together these pieces, a "risk assessment" then involves identifying, evaluating, and prioritizing the level of risk associated with potentially negative impacts. Keep in mind that a necessary piece of the assessment involves a recognition of what is deemed an acceptable level of risk for the organization. This requires a knowledge of your organization's tolerance for risk (also known as the "risk appetite").

For instance, consider the topic of handheld devices. Is there a tolerance for these to be personal and not owned by the organization? Ultimately, the keys to determining what drives that tolerance will be found in your organization's vision, mission, values, and culture.

Where patient privacy is concerned, a risk assessment will involve an examination of the human, natural, and environmental threats to an organization's processes and information systems that house private patient information.

Why Do It

The job of the privacy professional is to establish an effective system to protect sensitive patient information—also known as protected health information (PHI) or personally identifiable information (PII). The goal of a privacy risk assessment is to help determine where best you can allocate your available resources in order to achieve the highest level of protection.

If one were to try to eliminate each and every privacy risk, the cost—in time, effort, and financial assets—would be enormous. Therefore, a system is needed to help prioritize which risks must be addressed. In addition, organizations don't have unlimited resources, so the risk assessment will allow the organization to allocate its limited resources.

In fact, the assessment and management of privacy risks are so important, they're among the requirements spelled out in HIPAA. Specifically, the Security Rule requires that organizations:

- "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate"[2]; and
- "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [45 C.F.R. § 164.306(a)]."[3]

Furthermore, the Privacy Rule requires that organizations:

- "Must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information"[4];
- "Must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the [Privacy Rule]"[5];
- "Must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure"[6]; and
- "Must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate."[7]