Compliance Today - June 2019
The compliance role of the privacy and information security professional

By Marti Arvin

Marti Arvin (marti.arvin@cynergistek.com) is an Executive Advisor at CynergisTek in Austin, TX.

In today's world, the responsibility for information security and privacy compliance could be in one of any number of offices in an organization. The privacy officer and/or the information security officer (ISO) may report to the chief compliance officer (CCO). Either or both of these roles might report to the chief information officer (CIO). Yet another reporting structure is an independent report to the chief executive officer (CEO) or the governing body. In some organizations, one individual might have both roles. In other organizations, the CCO might also be named the privacy officer and/or the ISO.

Where the positions report to can be important, depending on the culture of the organization, but the key is that the roles have the support to actually perform the necessary oversight. It is also important to understand the responsibility of the roles.

Compliance with the Heath Insurance Portability and Accountability Act (HIPAA) is often the primary focus of the privacy officer or ISO, but it may not be the only focus. When an organization is an academic medical center with privacy oversight that includes the university, the privacy official may also have oversight for compliance with the Family Educational Rights and Privacy Act (FERPA) as well as other laws and regulations. In a healthcare organization, the security official is often looking at a broader scope for compliance than just HIPAA, such as evaluating the organization's information security posture against the National Institute of Standards and Technology (NIST) Cybersecurity Framework. However, HIPAA actually mandates these positions for covered entities. The HIPAA Privacy Rule requires that a covered entity designate a privacy official[1] and the HIPAA Security Rule requires the designation of a security official.[2]

Understanding the responsibilities of these roles as an oversight function can sometimes be lost. In some, particularly smaller organizations, the privacy official might also be the health information management (HIM) professional or have another role. It is equally common to see the ISO as a role within the information technology (IT) infrastructure of an organization. This can cause the oversight function of the role to be lost, because the individual is pulled in to an operational role to actually develop, implement, and run the information security function of IT. A key factor to having a successful oversight function is that the individual has the resources and the independence to carry out oversight. If that exists, having these dual roles is not an issue. However, that is often not the case.

When the privacy official is also the HIM director or has another role, the individual may not have the time to perform the necessary oversight functions required to be effective. Being a HIM director is, by itself, often a full-time job. The same can be true if the ISO is trying to perform oversight while simultaneously engaging in operational activity in the IT department. As such, the organization should not simply give someone the title of privacy officer or ISO. If an individual is given one or both of these titles, they need to insist on having the resources to actually carry out the functions.