COSMOS
Navigate the Compliance Universe

Compliance Today - February 2019
Security risk audits and risk mitigation plans to protect PHI

By Gerry Blass

Gerry Blass (gerry@complyassistant) is President and CEO at ComplyAssistant in Iselin, NJ.

- linkedin.com/in/gerry-blass-917a482

In today's fast-paced world, there is no limit to the number of risk areas that can be identified during a security risk audit. And, performing the audit is not enough. Healthcare organizations must establish rigorous controls and governance to mitigate identified risks.

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities and business associates conduct periodic risk assessments and implement risk mitigation plans. A risk assessment helps organizations ensure compliance with HIPAA's administrative, physical, and technical safeguards, and helps expose areas where an organization's protected health information (PHI) could be at risk.[1]

Although healthcare organizations are required to perform periodic risk assessments, they are not required to proactively prove that they have done so. Typically, an organization's assessment process is uncovered in one of two situations:

1. The organization has had a significant reportable breach. When this happens, there will likely be an investigation by the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR). The OCR will request to see key documentation, such as when the last risk assessment was performed, what risks were mitigated in risk-level order, what HIPAA policies and procedures are in place, what evidence of key activities is documented (e.g. workforce training), and what protocols and controls were in place at the time of the breach.[2]
2. The OCR decides to perform a random audit based on current audit protocols.

This article outlines the case for conducting periodic security risk audits—going far beyond the required assessment. An organization's primary motivation should be protecting the patients and itself. Passing an assessment is only one step in the process. Every organization must be keenly aware of high-risk areas and implement a proactive plan to address those risks.

What is the purpose of a security risk audit?

Let's first distinguish between "security risk audit" and "security risk assessment." These terms are often used interchangeably, but an audit is considered to be more intensive and comprehensive. Security risk assessments generally consist of a questionnaire on which the organization simply documents "yes" or "no" to indicate whether security protocols are in place. Alternatively, a security risk audit takes a more comprehensive approach. In addition to the questionnaire, an audit delves deeper into the actual policies and procedures in place and, most importantly, gathers documented evidence of the same.

At the highest level, the purpose of a security risk audit is to identify any and all locations where PHI is in use, in

transit, and at rest, and to determine what controls are in place to protect it.

PHI can be located in nearly every corner of a healthcare organization. Some examples include email, hardcopy, workstations, servers, databases, remote data centers, remote access, Wi-Fi, mobile devices, networks, and with people—both employees and contractors.

Types of controls to safeguard PHI include workforce education and phishing exercises; encryption for emails, mobile devices, and Wi-Fi; and security operations center (SOC) monitoring; honeypots used to draw potential attackers from a genuine target; and use of locked down ("dumb") terminals that are unable to store data on a local drive.