COSMOS
Navigate the Compliance Universe

Compliance Today - November 2019
Avoid recreating the wheel: Transparency in risk mitigation

By Gerry Blass and Jason Tahaney

Gerry Blass (gerry@complyassistant.com) is President and CEO at ComplyAssistant in Iselin, NJ. **Jason Tahaney** (jtahaney@hhsnj.org) is Director, Information Technology at Hunterdon Medical Center in Flemington, NJ.

- linkedin.com/in/gerry-blass-917a482/
- linkedin.com/in/jason-tahaney-91653618/

Did you know a typical healthcare system might perform up to 22 different types of security risk assessments each year? If the system uses a decentralized model, the assessment information is most likely gathered from a wide variety of areas—siloed, and not necessarily actionable. Although the organization is performing due diligence to adhere to the HIPAA Security Rule, is it doing its best to manage risk and resources? Probably not.

Whether or not healthcare organizations are prepared to perform a security risk assessment (SRA) each year, it is a required part of the HIPAA Security Rule[1] and should cover:

- Size, complexity, and capabilities of the covered entity;
- The covered entity's technical infrastructure, hardware, and software security capabilities;
- The probability and criticality of potential risks to electronic protected health information (ePHI); and
- The costs of security measures.

Unfortunately, healthcare organizations face immense challenges in performing security risk assessments and actually mitigating risks that are discovered, including:

- A high volume of risk areas, both inside and outside the four walls of a hospital;
- Increasing complexity of new, connected technologies;
- A siloed approach to risk assessments;
- A lack of transparency or understanding of risk across an enterprise; and
- Decentralized or unstructured risk ownership.

Because of these challenges, healthcare organizations may be spinning wheels and wasting time, energy, and money trying to make sense of the results of their annual security risk assessments. Imagine if one department discovered and mitigated a data security risk, but another department with the same or similar risk was not aware of the other department's efforts, and thus created its own risk management project. There is no need to recreate the wheel every time.

This article explores practices to make annual security risk assessments more transparent and actionable to reduce overall enterprise risk.

Manage risk across silos using a risk register

When performing SRAs, healthcare organizations typically end up with several disparate risk reports from different areas, including meaningful use, credit card processing, finance, security operations, third-party vendors, facilities management, cloud services, and both acute and nonacute care sites. Perhaps the SRAs are even performed by different teams, contributing to inconsistency in how the assessment data is gathered and reported.

With dozens of departments and corresponding assessments, you can imagine the difficulty of making truly informed decisions on how to prioritize and manage risk in ways that make the most sense for the enterprise as a whole.

With the assistance of a risk management committee, take the time to consolidate the results of each assessment into a single repository—a risk register. This risk register will be your single source of truth moving forward. Using it, you can:

- Visualize common risk across departments,
- Plan and prioritize risk mitigation, and
- Be more transparent with senior leadership.