COSMOS
Navigate the Compliance Universe

Health Care Privacy Compliance Handbook, 3rd Edition
10. Auditing and Monitoring for Privacy in Healthcare

By Sheryl Vacca, CHC-F, CHPC, CHRC, CCEP-F, CCEP-I[1]

Executive Summary—Key Steps

- Agree on a common framework for the risk-based auditing and monitoring program.
- Assess privacy risks across the enterprise and then prioritize them by looking at the likelihood of occurrence and impact for the organization.
- Develop a risk-based auditing and monitoring plan or integrate into current compliance plan from the identified privacy risk priorities.
- Assure that a management action plan is developed to mitigate risks and/or resolve risks in a timely manner.
- Assess auditing and monitoring process for effectiveness.

Getting Started

In designing the privacy risk-based auditing and monitoring activities, it is important to work closely with the organization's senior leadership and the board, or committee of the board, to gain a clear understanding of auditing and monitoring expectations and how these activities can be leveraged together to help minimize and mitigate privacy risks for the organization. The organization's compliance officer should be included as well to assure that applicable resources are leveraged and auditing and monitoring activities for privacy are not duplicated in the organization's overall compliance plan. There may be other functions that might not be represented on the senior leadership team with whom you will want to consider discussing these activities as well.

Processes for establishing the privacy risk-based auditing and monitoring plan should include:

- Performing a risk assessment
- Prioritizing the identified risks
- Developing the plan

If privacy is part of the overall comprehensive compliance plan, then it would be considered in the risk prioritization and ranking for the compliance plan. The overall goal of the plan is to perform periodic audits and monitoring to determine compliance with respect to applicable regulatory and legal requirements, organizational policies, and/or laws. An additional goal of the plan should be to provide assurance that management controls are in place for the detection and/or prevention of noncompliant behavior. Additionally, risk-based auditing and monitoring should include mechanisms to determine that management has implemented corrective action to mitigate or resolve any privacy risks identified.

Once the common framework for the risk-based auditing and monitoring program has been established, six key tasks must be performed:

1. Assess and prioritize privacy risks.
2. Develop a risk-based auditing and monitoring plan.
3. Execute the plan.
4. Facilitate management's response to the corrective action plan to mitigate and/or resolve risks.
5. Follow up with management to determine resolution and/or mitigation of the risks identified. This might include re-auditing, validation, monitoring, or other focused activities to assist with determination of whether the risk has been decreased.
6. Assess and evaluate the overall process for effectiveness.