The role of the chief audit executive (CAE) is more critical and challenging than ever, especially in healthcare settings. CAEs working in hospitals, health systems or other provider settings must navigate risks in an era of transformation, while building adequate assessments into their internal audit plans. The decentralized structure of some healthcare institutions and lack of resources add to the complexity.

The following is a collection of insights documented over the past year at Association of Healthcare Internal Auditors (AHIA) CAE roundtables that took place in Arizona, California, Texas, New York and Pennsylvania.

So what is on the mind of today’s healthcare CAE? Here are the three most common key challenges and insights summarized from our discussions.

Enterprise Risk Management (ERM) is a key concern, but few organizations are undertaking formal ERM assessments

CAEs have considerable interest in ERM for good reason. However, they have questions about the best way to incorporate ERM results into internal audit planning, and about the difference between Risk Assessment and ERM.

Only one in eight participants at the roundtables had conducted an ERM assessment. CAEs agree doing an ERM assessment is a good idea, but expressed concerns that turning ERM into an ongoing process might be hard to justify in terms of its cost and perceived value.

Many potential benefits of conducting an ERM assessment were discussed, including:

- Creating a common definition of risk
- Potential for reducing the number and impact of surprises
- Management’s attention gets focused on the most critical risks
- Stakeholder confidence and value is increased

Managing threats to data security and privacy is a growing need

CAEs are growing increasingly concerned about how to effectively manage risks related to data security and data privacy. For example, CAEs note technology risks and cyber security threats from cloud computing. Healthcare organizations’ widespread initiatives in Electronic Health Records (EHRs) also increase hospitals’ requirements related to ensuring electronic Protected Health Information (ePHI), and weigh heavily on the minds of CAEs.

Moreover, increased audits and enforcement related to the EHRs and ePHI from the Office for Civil Rights (OCR) are a growing concern. OCR investigators are beginning to audit healthcare organizations concerning the establishment of and adherence to privacy and security practices for safeguarding health information and data breach notification standards. The OCR audits are called for under the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Also high on the list of data security headaches for CAEs are mobile technology devices. Keeping an accurate inventory of devices, encryption and potential information breaches are becoming challenging issues. Some CAEs report all of their organization’s devices are encrypted, while others say encryption software slows down devices such as desktops and makes it harder to use them.

Inventorying these devices is a challenge. Nearly a constant issue, according to
roundtable participants, is making sure employees keep the new devices, such as IPads, IPhones and laptops, appropriately encrypted.

CAEs noted the following best practices and worthy considerations related to data security and privacy:

1. Conduct a technology risk assessment, plus an IT internal audit and security test.
2. Consider IT security in research facilities.
3. Examine vulnerabilities that reside with access to patient billing information and functions.
4. Review the types and format of information leaving the hospital with vendors.
5. Data security extends beyond systems to include private information kept in hard copy sources (such as written credit card information, personnel files, etc.).
6. Be aware of other devices that contain ePHI (e.g. medical devices, copiers).
7. Look into document retention and destruction policies.
8. Understand the reviews your institution performs to determine inappropriate access to medical records.
9. Be on the lookout for the use of mobile phones and built-in cameras. More than one phone/camera-related incident has ended in lawsuits and state’s attorney inquiries.
11. Follow up HIPAA refresher training with flagged individuals and their supervisors.
12. Be sure to provide training to new employees and to the staff of acquired practices.

One critical factor to keep in mind is that data privacy and security involves a heavy dose of employee training and education. It is vital to implement mandatory training and maintain records demonstrating that each employee has completed the required training, such as electronic receipts, surveys and self-education. One CAE stated that employees at his organization who failed to attend a mandatory training were suspended without pay.

It was noted that training is most effective when it is designed to reach multiple audiences—especially those with less on-the-job experience, such as recent college graduates.

Keep the teaching methods interesting. For example, most audiences will relate better to a discussion centered on storytelling, rather than intricate explanation of policies. One thing is clear: whether you perform these tasks in-house or outsource them, it is important that you train before a security breach forces you to do so.

Social media poses significant risks

Social media is transforming how consumers interact with corporations, governments, traditional media and each other—and healthcare internal auditors have not failed to notice. Some hospitals have terminated employees over use of social media.

Multiple risks are connected to social media. Organizations no longer control the message, since now any stakeholder can share information or opinion instantly through uploaded text, images, audio and video content.

The primary reason for medical students to be in the facility is to learn, and now they can easily access patient information, which could pose a significant risk. Moreover, the line between academic need and patient privacy can create uncertainty regarding appropriate use.

While institutions are grappling with where to draw the line when it comes to oversight of personal communication, all roundtable participants strongly recommended having a social media policy. Having effective education and policies in place about social media use will lessen risks. However, to date,
few institutions reported having a comprehensive social media policy. Even fewer organizations are training employees about social media risk exposure.

The important areas to cover in a social media policy include:

- Prohibition on inappropriate cell phone use, e.g., sharing pictures of patients taken with cell phone cameras or other private information
- Prohibition on communicating with or about patients on Facebook, mentioning them on blogs or other social media venues
- Prohibition on describing patient scenarios (even anonymously)
- Prohibition on giving advice on blogs

Does your organization have a social media policy?

Is your organization training employees and doctors on how to deal with social media?

Conclusion

The internal audit function of any healthcare institution is particularly critical in today’s regulatory environment, given public policymakers’ focus on the significant cost of healthcare, along with each organization’s response to shrinking reimbursement and volumes. Improprieties will be grounds for more investigations in the future, and many operational issues, such as reimbursement, supplier and distribution relationships, and marketing and pricing strategies, will be tough to root out without strong internal auditing. Effective CAEs will focus on addressing issues quickly because this will help healthcare systems respond assertively to any potential accusations of impropriety. Ultimately, the value delivered by internal audit will ripple through to the entire healthcare organization.

Forums such as AHIA roundtables enable CAEs to share best practices with peers, helping to bring well-deserved peace of mind to the challenges healthcare internal audit executives face today. NP

To learn more about AHIA-hosted Chief Audit Executive Roundtables, you may contact the authors.

Authors

Bob Lund, CPA, is Director of Audit Services for Banner Health. You may reach him at (602) 747-4603 or Robert.Lund@bannerhealth.com.

Mark Oster is Partner in Charge, Health Care Business Advisory Services, Grant Thornton, LLP. You may reach him at (212) 542-9770 or Mark.Oster@us.gt.com.

Donna Wachman is National Marketing Manager, Grant Thornton LLP. You may reach her at (704) 632-3521 or Donna.Wachman@us.gt.com.

“I’d like to give you a raise and promotion, but that wouldn’t be fair to others who don’t stay late or work as hard as you.”