HIPAA Risk Analysis: OCR-Quality Audits

Another opportunity to provide assurance to leadership

By Bob Chaput, MA, CISSP, CRISC, HCISPP, CIPP, and Mary Chaput, MBA, HCISPP, CIPP, CIPM

With the emergence of electronic health records, there has been a corresponding increase in the number of threats to patient health information and potentially to the actual health of patients. The vulnerabilities resulting in data breaches can be the cause of significant financial and reputational repercussions for organizations that have not undertaken effective preventative preparations.

Bob Chaput is the CEO of Clearwater Compliance, LLC, and is one of the industry's leading authorities in healthcare information security today. Bob has supported hundreds of hospitals and health systems in successfully manage healthcare's evolving cybersecurity threats and ensure patient safety. You can contact him at Bob.Chaput@clearwatercompliance.com.

Mary Chaput is the CFO and CCO of Clearwater Compliance, LLC. She has 35 years of operational management and financial experience for publicly traded companies in the information services and healthcare industries. You can contact her at Mary.Chaput@clearwatercompliance.com.

Boards are realizing an information risk management (IRM) program grounded on a comprehensive risk analysis needs to be established under the watchful eyes of an autonomous and process-oriented function. Additionally, the risk analysis must meet the emerging Office of Civil Rights (OCR) standard of care; that is, it needs to be "OCR quality."

Many organizations are expecting internal audit to integrate this broader spectrum of IRM into their audit programs. Yet, according to an annual survey by Protiviti published in March 2016, 27 percent of the over 1,300 responding internal auditors and audit executives reported that information or cybersecurity risks are not yet included as part of their internal audit plan—including 11 percent that have no plans to include it.

The hesitancy of some senior management and boards to include IRM in the scope of internal audit functions may be influenced by internal audit's historically narrow scope of accounting and compliance audits, compared to the complexity, depth and breadth of information risks. In fact, the Protiviti survey highlighted that the lack of skills and software tools contributed to the inability of organizations to adequately address cybersecurity risks.

Internal auditors can take advantage of their experience and discipline to help assure risk analysis methodologies and output meet the IRM and regulatory compliance needs of the organization. The following is a specific audit approach and tool for evaluating and auditing a risk analysis in line with the HIPAA Security Rule, recommendations from the National Institute of Standards and Technology (NIST), and guidance from OCR.

Leverage internal auditors' competencies

A competent and persuasive evaluator of financial and compliance programs has historically undertaken these actions:

1. Implementing and maintaining an efficient and effective audit framework

2. Evaluating the consistency of actual practices with respect to internal policies and procedures and external regulatory requirements

3. Evaluating the potential impact of inaccuracies and noncompliance

4. Identifying and reporting weaknesses in processes

5. Monitoring approved remediation activities as part of the structured processes

6. Recommending overall risk strategy for board approval

Competency in these areas can be leveraged to expand the scope of internal audit's responsibilities to include risk analysis and IRM, thereby providing assurance to leadership that information risks are appropriately identified, evaluated and managed.

The challenges of IRM

The safeguarding of health information can pose challenges to compliance auditing. These include:

1. Increasing threats due to the value of stolen health information

2. Use of private and public cloud computing platforms

3. Exploding consumer adoption of wireless, portable, connected devices

4. Expanding dissemination of health information to a myriad of service providers

5. Emerging technologies such as biomedical devices that more directly endanger patient safety

6. Proliferation of "shadow IT" solutions outside the purview of IT

7. Increased ability to disrupt or bring harm to organizations (e.g. for competitive purposes)

8. Complex, ever-evolving Internet of Things

Fifty-two percent of respondents to the Institute of Internal Auditors Pulse of Internal Audit 2016 survey reported that a "very high" or an "extreme" lack of cybersecurity expertise among internal audit staff affects internal audit's ability to address cybersecurity risk.

Although still relevant, the audit focus is no longer just on the effectiveness and consistency of practice for workforce procedures and training. A structured approach to IRM and risk analysis must be established to enable internal audit to apply the skills and experience the organization relies on while providing themselves with the knowledge needed to be effective and efficient in this expanded role.

IRM and risk analysis

To audit an IRM program, an understanding of the objective and the details of the IRM and risk analyses processes is critical. The risk that is being evaluated is the potential compromise of the confidentiality, integrity, and/or availability of health information given the controls that are in place to protect it. Not only are such compromises potentially reportable under HIPAA Breach Notification Rule requirements, more importantly they may represent patient health and safety issues.

Potential compromises of health information

What if health information is shared or accessed inappropriately? – Impermissible uses or disclosures of sensitive information constitute a compromise of confidentiality. These types of breaches may be perpetrated by hackers who sell the information on the black market or by employees who misaddress faxes, for example.

This type of compromise can also be the result of snooping, an activity most common in celebrity-visited hospitals, or in healthcare settings where those with medical record access may know patients personally. Depending on the sensitivity of that health information, such disclosures can result in significant physical, emotional, reputational, financial or legal harm to the patient and significant financial and reputational harm to the organization.

What if health information is not complete, up to date and accurate? – Unauthorized deletion or modification of sensitive information is a compromise of the integrity of the information and may be caused by an intentional attack to

change someone's vital data or an accidental change by a clinician or administrative staff member.

Unauthorized changes made in health records can, for instance, include changes to blood type, medication dosages, or allergies. Such unauthorized changes or deletions can result in patient safety issues, including incorrect diagnoses, prescriptions or treatment, and even death.

What if health information is not there when it is needed? – With the implementation of electronic medical records, providers and patients expect health information to be available whenever and wherever it is needed. If health information is not available, diagnosis or treatment may be delayed and/or result in errors in medical decisions. Threats to information availability can arise from environmental events (e.g., hurricanes) or structural occurrences (e.g., equipment failures) as well as adversarial incidents such as ransomware attacks.

How can internal audit help?

There are typically three tiers to the business risk management process—strategic, tactical and operational. Internal auditors are familiar with this hierarchy. In IRM, the tiers require the following attention:

- *Strategic* – Organizations must develop an IRM framework and strategy for board approval, making it a meaningful C-suite and board agenda item.
- *Tactical* – Organizations must establish, implement and mature an organization's IRM program consistent with the framework and strategy.
- *Operational* – Organizations must assess the authenticity and comprehensiveness of a comprehensive information risk analysis process and results.

Auditing should be performed at all three tiers. The focus with respect to this article is on operational audits—specifically reviews of the foundational information risk analysis process and results.

The objective of IRM

Once the framework and strategy are established, a comprehensive risk analysis is completed. This risk analysis step must be conducted to identify and evaluate all risks to an organization's information assets.

Risk response must then be determined and implemented to accept, avoid, mitigate or transfer those risks. Risk analysis and risk response are two critical steps in an overall IRM program. These steps are followed by ongoing risk management program monitoring.

Starting with an operational foundation, according to The Institute of Internal Auditors, an IRM audit program should include:

- Giving assurance and evaluating the risk management processes
- Giving assurance that risks are correctly evaluated and key risks identified
- Reviewing and reporting on the management of key risks

Fundamentals of an information risk analysis process

Identifying risk

The existence of risk means there must be the possibility (threat) of loss or harm to an asset (in this case, to patient information and/or to the organization). Threats to this asset must exist, and there must be a vulnerability that the threat may exploit.

Only when there is an "asset-threat-vulnerability" is there a risk that requires analyzing. As a simple example, a laptop with ePHI is an asset/media type that has a threat of being stolen and the ePHI accessed. A vulnerability may be a weak password. The laptop-thief-weak password risk needs to be analyzed. Similarly, a laptop-shoulder surfer-absence of privacy screen risk would need to be analyzed. There will be many of these triplet groupings to analyze if the risk analysis is comprehensive.

Rating risk

To determine the level of risk once each triplet is identified, you must consider the likelihood of the threat exploiting that vulnerability and the impact to the organization if it were to happen. When the likelihood of a risk is high and the impact is high, the risk rating should be considered critical for the organization. It is then necessary to remediate with the implementation of controls and/or safeguards to reduce the likelihood and/or impact.

The output of the risk analysis process is a risk register that includes a risk value assigned to each of the triplet risks identified. The level or value of the risk rating guides the decision on risk response called for in the HIPAA Security Rule under risk management.

You're not alone

Internal auditors who are unsure of the requirements of an information risk analysis are not alone. Data from the OCR shows that few organizations are conducting risk analysis properly:

- 68 percent (29 out of 42) of the 2012 OCR Phase I auditees had failed to conduct a risk analysis.

- 71 percent (30 out of 42) of healthcare organizations that entered into resolution agreements and corrective action plans with OCR were cited for failed risk analysis (6 in 2016 so far).[1]

- 63 percent (27 out of 42) have not established a comprehensive risk management program and process.

Both risk analysis and risk management are required by the HIPAA Security Rule and are the foundation of any IRM program. Yet much uncertainty and misinformation surrounds what constitutes an OCR-quality risk analysis.

The risk analysis dilemma

Conducting a comprehensive risk analysis can be daunting, considering the number of combinations of information assets/media, threats, vulnerabilities and controls that may apply. Commonly, when conducted properly, hundreds and even thousands of unique triplets or risks are identified.

To truly understand all the possible ways in which a compromise may occur, all ePHI in every information asset, in every facility or line of business (such as clinics, hospitals, hospice, insurance, home health, etc.) must be assessed against every relevant threat and vulnerability. Then a risk value must be determined for each based on the effectiveness of the safeguards and controls that are currently in place.

> The lack of skills and software tools contributed to the inability of organizations to adequately address cybersecurity risks.

If the number of information assets and media, threat sources, threat actions, vulnerabilities and controls were each limited to only 10 possibilities, there would be 10^5 or 100,000 considerations for an organization to assess. It is no surprise that organizations struggle to complete this work properly and comprehensively. The good news is that there are cutting-edge software solutions that streamline the risk analysis process.

Process and results

Internal audit often relies on control checklists, such as a FISMA (Federal Information Security Management Act), ISO27000 or NIST SP800-53 controls. But controls are simply one of the factors in conducting risk analysis. Risk analysis is about safeguarding your assets, not relying on someone's generic controls checklist.

To audit your HIPAA Security Risk Analysis, it may be better to use the following ten Risk Analysis Key Essential Criteria and determine their rigorous completion.

1. *Scoping* – All ePHI that an organization creates, receives, maintains, or transmits must be included in the risk analysis.

2. *Collecting data* – The data on ePHI gathered using these methods must be documented.

3. *Potential threats and vulnerabilities* – Organizations must identify and document all reasonably anticipated threats to ePHI and vulnerabilities.

4. *Current security measures* – Organizations must assess and document the security measures an entity uses to safeguard ePHI.

5. *Likelihood of threat occurrence* – The Security Rule requires organizations to assess the likelihood of potential risks to ePHI.

6. *Potential impact* – The Security Rule also requires assessment of the impact, of potential risks to confidentiality, integrity and availability of ePHI.

7. *Level of risk* – The level of risk must be determined. For example, analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence.

8. *Finalizing documentation* – The Security Rule requires the risk analysis to be documented.

9. *Periodic reviewing and updating* – The risk analysis process must be conducted on an ongoing basis.

Meeting emerging OCR standard of care

The risk analysis should be examined against the specific requirements in the HIPAA Security Rule, the explicit guidance provided by OCR in July 2010, the current OCR Audit Protocol and NIST Special Publication 800-30.

For organizations interested in completing a rigorous self-review of their current HIPAA security risk analysis process and results, a complimentary audit tool titled "Clearwater OCR-Quality HIPAA Risk Analysis Self-Review™"[2] may be of help.

[1] www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/

[2] www.surveygizmo.com/s3/2888991/OCR-Quality-HIPAA-Risk-Analysis-Self-Review

The ten Risk Analysis Key Essential Criteria are derived from these references:

1. HIPAA Risk Analysis implementation specification language at 45 CFR §164.308(a)(1)(ii)(A) and (B) of the HIPAA Security Rule (www.hhs.gov/hipaa/for-professionals/security/)
2. Methodology outlined in the HHS/OCR "Guidance on Risk Analysis Requirements under the HIPAA Security Rule" (www.hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html)
3. Underlying NIST Special Publications for performing a risk assessment and, specifically NIST SP 800-30 "Guide for Conducting Risk Assessments" (http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf)
4. Documentation found in OCR investigation letters and "OCR Resolution Agreements/Corrective Action Plans" (www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html)
5. OCR Audit Protocol, updated April 2016, specific to risk analysis and risk management (www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/)

Conclusion

You cannot do this on your own, nor should you. Accountability for risk management is rightfully the responsibility of the executive team, who can establish and expand the authority of a governance and oversight body in ways that include:

1. Formalizing the IRM program
2. Assigning responsibilities to cross-functional teams for identification, classification and remediation of risks to information assets
3. Approving and supporting the IRM framework and process
4. Establishing the risk appetite of the organization
5. Making informed decisions on risk response
6. Ensuring adequate resources to implement successfully

According to Protiviti's survey, there are two critical factors when establishing and maintaining an effective cybersecurity plan: a high level of engagement by the board of directors with respect to information security risks, and evaluating cybersecurity risk in the current audit plan. The internal audit function can take an important leadership role in these two areas. Start by carefully auditing your current risk analysis to determine if it is indeed of OCR quality. **NP**

Spear Phishing and Ransomware – continued from page 25

---

3. Protect your workspace: At any given moment, your desk may contain notes or documents that contain confidential information, or you might have sensitive information displayed on your computer monitor.
4. Don't open attachments: Unless you are absolutely sure from whom the email came and what the attachment contains, do not open or execute an attachment.
5. Keep your virus detection device turned on: Antivirus scanning is only effective if it is turned on.
6. Do not install unapproved software: Downloading software from the Internet is a primary source of viruses, spyware and Trojans, and even legitimate software may not be compatible with other software on your computer and could cause conflicts.
7. When in doubt, call the help desk: It is better to contact your internal resources to check it out than to be the cause of the attack that takes down the corporate network. Finally, if you are suspicious of something or something just seems a little off, disconnect from networks immediately.

Conclusion

The threat of ransomware continues to expand, and attention is on the healthcare industry. The more successful these attacks are, the more attacks there will be. You can help your organization protect itself by learning how hackers get into systems and ensuring that your organization has preventative controls in place. **NP**