Security Risk Analyses Can Offer Significant Findings

Save to myBoK

By Wes Morris, CHPS, CIPM, HCISPP, and Sandra Nunn, MA, RHIA, CHP

ONE OF THE critical information governance (IG) functions is successful execution of an organization's privacy and security responsibilities. Chief among these responsibilities is to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI). This assessment is a foundation upon which other security processes will depend. Poor or non-existent risk analysis processes have been a finding in 89 percent of settlement agreements and civil money penalties imposed by the US Department of Health and Human Services' Office for Civil Rights (OCR). In 2018 alone, the cost was over $24 million for organizations that failed to implement effective risk analysis or risk management processes.

The intent of this article is to help healthcare entities consider a strategy for a security risk analysis process, considering current requirements and industry best practices for protecting ePHI. Depending on the risk profile and resources, some recommendations and decisions will require significant research, analysis, policy development, investments, and approvals.

It is critical to understand that a risk analysis is not a non-technical evaluation required by HIPAA's Evaluation Standard. Risk analysis is required by HIPAA's Security Management Process Standard and is a process of identifying the vulnerabilities in the entity's networks, computer systems, personnel processes, physical security, and environment that could be exploited by a threat agent (whether human or environmental). A risk analysis also considers the likelihood and impact to the organization if the vulnerability were exploited.

OCR's guidance on risk analysis requirements under the HIPAA Security Rule describes nine essential elements of a risk analysis, regardless of the methodology:[1]

1. Scope: All ePHI that an organization creates, receives, maintains, or transmits must be included.
2. Data collection: The data on ePHI gathered using these methods must be documented.
3. Identify potential threats and vulnerabilities: Reasonably anticipated threats to ePHI must be identified and documented.
4. Assess current security measures: The security measures used to safeguard ePHI must be included.
5. Determine the likelihood of threat occurrence: Consider the probability a threat will occur.
6. Determine the potential impact of threat occurrence: Address the impact to confidentiality, integrity, and availability of ePHI.
7. Determine the level of risk: The level could be determined by combining the values assigned to the likelihood and resulting impact of threat occurrence.
8. Finalize documentation: The risk analysis must be documented, but no specific format is required.
9. Periodic review and updates to the risk analysis: Update and document security measures "as needed."

A risk analysis project should establish the scope and required actions (i.e., what the project will entail) and the end goal and desired state. Once addressed, a timeline based on resources and end goals can be established. AHIMA suggests the following risk analysis framework.

Risk Analysis Framework

Start with a system characterization. Create an inventory of applications and systems that involve ePHI. Then group assets as applications (electronic health records (EHRs), lab or radiology information systems (LIS/RIS), enterprise content management, etc.) or systems (workstations, laptops, networks, etc.).

Next, identify reasonably anticipated threats. Consider:

- Environmental factors (i.e., power failures, chemicals, or liquid leakage)

- Acts of man (i.e., intentional or unintentional actions causing loss of ePHI)
- Acts of nature (i.e., wildfires or flooding)

Then conduct a vulnerability assessment. Organizations should assess:

- Missing controls. Examples:
    - Use of mobile devices without a mobile device management solution
    - No encryption methodology
    - No reviews of activity in information systems
- Identify how applications or systems could be exploited. Examples:
    - Unpatched applications could be exploited
    - ePHI on a stolen device could be accessed by an outsider

When conducting a control assessment, organizations should assess what controls are in place currently. Is there protection of a data center from flooding and fire threats? Malware protections? Daily backup of all ePHI systems?

Next step in a risk assessment is the risk likelihood determination. Decide the probability of each threat occurring. For example, the likelihood of a staff member clicking on a link within an email, or a laptop being stolen from a vehicle.

Conduct an impact analysis. Rate possible impacts from low to very high and evaluate what the risk would do to the organization. For example:

- The EHR goes down and cannot be restored for three days—Risk: high
- The billing system is attacked by ransomware and payment demanded for a decryption key—Risk: medium

AHIMA's Impact Definitions

Magnitude	**Definitions of exploitation of the vulnerability**
Very High (16)	(1) May result in the high costly loss of major tangible assets or resources; (2) May violate, harm, or impede an organization's mission, reputation, or interest significantly, or (3) May result in human death or serious injury.
High (8)	(1) May result in the costly loss of major tangible assets or resources; (2) May violate, harm, or impede an organization's mission, reputation, or interest significantly; or (3) May result in serious human injury.
Medium (4)	(1) May result in the costly loss of tangible assets or resources; (2) May violate, harm, or impede an organization's mission, reputation, or interest; or (3) May result in human injury.
Low (2)	(1) May result in the loss of some tangible assets or resources; or (2) May affect an organization's mission, reputation, or interest noticeably.

Likelihood of occurrence	Definitions
Almost Certain (5)	Constant or frequent
Likely (4)	May happen once a year
Moderate (3)	May happen once in 5 years
Rare or unlikely (1 or 2)	May happen once in 10 years

See the sidebar above that lists AHIMA's impact definitions based on magnitude and definitions of exploitation.

Risk determination should be factored as part of the risk assessment, and can be calculated using the formula: Risk = Likelihood * Impact. A high impact (16) multiplied by a high likelihood (4), yields a risk score of 64, whereas a low impact (2) multiplied by a high likelihood (4) yields a risk score of 8. This calculation allows placing of limited resources to target the high risks first. Also, recommended controls should be determined. Provide recommendations to manage risks appropriately. For example: Implement training on how malware can be introduced through email links; encrypt laptops to minimize access in case of theft; limit access to server rooms and secure areas.

After the analysis is complete the results should be documented. Create a summary of key findings, recommendations, and estimates. The documentation should include a timeframe to implement needed changes as well as an assessment of financial and personnel resources needed to mitigate the identified risks.

For each documented risk a decision should be made to either:

- Reduce risk by implementing additional controls
- Transfer the risk
- Avoid the risk by removing the process or system
- Accept the risk

Risk Assessment Timeline

Contingent on the size and complexity of the healthcare entity, some of the following risk assessment actions can be done concurrently:

- One year to do an inventory of all organizational computer systems, applications, and networks
- One year to organize a digital asset function and to staff it
- One month to create a security assessment taskforce
- Two months to review existing HIPAA compliance provisions and to review new HIPAA requirements
- Six months to create an organizational risk assessment tool and questionnaire and distribute throughout the organization; development of a database to collect results of the questionnaires
- Two months to assemble, summarize, and analyze reported risk assessments from the components of the organization
- IG steering committee reviews threats, gaps, and recommendations and makes the decisions on organizational actions. IG committee provides funding and human resources to implement needed actions.
- One month: Security risk assessment taskforce transitions to ongoing security incident response group. Security policy and procedures developed through the stakeholder group listed below in conjunction with the IG committee.
- Ongoing workforce education and training on security management policies
- Ongoing auditing/monitoring of workforce adherence to policies and procedures

End Goal and Desired State

The end goal and desired state is to ensure availability and access to ePHI for optimal patient care while simultaneously protecting ePHI from impermissible access and disclosure. The stakeholders required to complete a risk assessment include: legal, privacy/security, risk management, compliance, IT, health information management, business unit leaders, and enterprise information management leaders or executives.

Benefits of Risk Assessments

Multiple benefits come from an effective risk assessment. When completed and acted upon, the assessment can plug security holes, prevent security breaches, and protect patient care capabilities.

Other benefits include:

- Enhance planning capabilities
- Justify spending based on potential recovery costs required due to breaches, failed audits, etc.
- Cost-effective compliance that meets multiple legal requirements, including HIPAA
- Accurate and controlled digital asset management
- Accurate and controlled management of IT licensing requirements
- Documentation of due diligence maintained

Patients, clinical teams, the breach response team, and IT staff all benefit from risk assessments since they prevent incidents. The entity's reputation, financial wellbeing, and continuous ability to provide acceptable access to PHI all benefit as well.

Note

1. US Department of Health and Human Services' Office for Civil Rights. "Guidance on Risk Analysis Requirements under the HIPAA Security Rule." July 14, 2010. www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.

Wes Morris (wes.morris@clearwatercompliance.com) is senior principal consultant for Clearwater Compliance. Sandra Nunn (casand74@msn.com) is principal at KAMC Consulting.

Article citation:
Morris, Wes. "Security Risk Analyses Can Offer Significant Findings." *Journal of AHIMA* 90, no. 3 (March 2019): 24–25; 51.