Risk Analyses vs. Gap Analyses – What is the difference?

April 2018

The Health Insurance Portability and Accountability Act (HIPAA) Rules require covered entities and their business associates to safeguard electronic protected health information (ePHI) through reasonable and appropriate security measures. One of these measures required by the Security Rule, is a risk analysis, which directs covered entities and business associates to conduct a thorough and accurate assessment of the risks and vulnerabilities to ePHI (*See* 45 CFR § 164.308(a)(1)(ii)(A)). Conducting a risk analysis assists covered entities and business associates identify and implement safeguards that ensure the confidentiality, integrity, and availability of ePHI. The purpose of this document is to explain the general differences between a risk analysis under the Security Rule's regulatory requirement and a "gap analysis."

In Brief:

- A risk analysis is a necessary tool to assist covered entities and business associates conduct a **comprehensive** evaluation of their **enterprise** to identify the ePHI and the risks and vulnerabilities to the ePHI. A covered entity or business associate may use the results of a risk analysis to make appropriate, enterprise-wide modifications to their ePHI systems to reduce risks to a reasonable and appropriate level.

  A gap analysis is typically a narrowed examination of a covered entity or business associate's enterprise to assess whether certain controls or safeguards required by the Security Rule have been implemented. A gap analysis provides a high-level overview of how an entity's safeguards are implemented and show what is incomplete or missing (*i.e.*, spotting "gaps"), but it generally **does not** provide a comprehensive, enterprise-wide view of the security processes of covered entities and business associates.

Risk Analysis:

The Security Rule does not require a specific methodology to assess the risks to ePHI nor does it require risk analysis documentation to be in a specific format. However, there are certain practical elements that, if incorporated into a covered entity or business associate's risk analysis, can assist in satisfying the regulatory requirement. These elements may include:

- **Calibrating Scope**
  Encompassing the potential risks to **all of an entity's ePHI**, regardless of the particular electronic medium in which it is created, received, maintained, or transmitted, or the source or location of its ePHI.
- **Collecting Data**
  Identifying locations and information systems where ePHI is created, received, maintained, or transmitted. This may include not only workstations and servers, but also applications, mobile devices, electronic media, communications equipment, and networks, as well as physical locations.
- **Identifying and Documenting Potential Threats and Vulnerabilities**[1]
  Identifying and documenting technical and non-technical vulnerabilities. Technical vulnerabilities may include holes, flaws, or weaknesses in information systems; or incorrectly implemented and/or configured information systems.
- **Assessing Current Security Measures**
  Assessing and documenting the effectiveness of current controls, for example the use of encryption and anti-malware solutions, or the implementation of patch management processes.
- **Determining the Likelihood and Potential Impact of Threats**
  Determining and documenting the likelihood that a particular threat will trigger or exploit a particular vulnerability, as well as the impact if a vulnerability is triggered or exploited.
- **Determining the Level of Risk**
  Assessing and assigning risk levels for the threat and vulnerability combinations identified by the risk analysis. Determining risk levels informs entities where the greatest risk is, so that entities can appropriately prioritize resources to reduce those risks.
- **Creating Documentation**
  Documenting the results of a risk analysis. Although the Security Rule does not specify a form or format for risk analysis documentation, such documentation should, as appropriate for the entity, contain sufficient detail to demonstrate that an entity's risk analysis was conducted in an accurate and thorough manner. If a covered entity or business associate submits a risk analysis lacking sufficient detail in response to an OCR audit or enforcement activity, *e.g.*, if a risk analysis lacks one of these elements, OCR may ask for additional documentation to demonstrate that the risk analysis was, in fact, conducted in an accurate and thorough manner.
- **Reviewing and Updating**
  Reviewing, conducting, and updating a risk analysis regularly. Although the Security Rule does not prescribe a frequency for performing risk analyses, a risk analysis process works most effectively when viewed as an ongoing process and is integrated into an entity's business processes to ensure that risks are identified and addressed in a timely manner.

[1] One definition of threat, from NIST (SP) 800-30, is "[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability." *Id.* Vulnerability is defined in NIST Special Publication (SP) 800-30 as "[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy." *Id*. Although the definitions of "threat" and "vulnerability" in the NIST guidelines do not apply to the regulatory requirements in the Security Rule, covered entities and business associates may find these definitions helpful and their content valuable when conducting a risk analysis.

Gap Analysis:

A gap analysis typically provides a partial assessment of an entity's enterprise and is often used to provide a high level overview of what controls are in place (or missing) and may also be used to review an entity's compliance with particular standards and implementation specifications of the Security Rule. A gap analysis may take a form similar to the example below.

HIPAA Regulation	Regulatory Summary	Policies & Procedures Documented?	Policies & Procedures Implemented?	Compliance Rating
45 C.F.R. § 164.308(a)(1)(ii)(B)	**Risk Management:** Implement security measures to reduce risks and vulnerabilities to a reasonable and appropriate level.	100%	50%	Not Compliant
45 C.F.R. § 164.308(a)(1)(ii)(C)	**Sanction Policy:** Apply appropriate sanctions against workforce members who fail to comply with security policies and procedures.	100%	100%	Compliant
45 C.F.R. § 164.308(a)(1)(ii)(D)	**Information System Activity Review:** Implement procedures to regularly review records of information system activity.	50%	50%	Not Compliant

A gap analysis similar to the above does not incorporate the above elements of a risk analysis and may not satisfy a covered entity or business associate's risk analysis obligations under the Security Rule because, for example, it does not assess the risks to ***all*** of the ePHI an entity creates, receives, maintains, or transmits (*See* 45 C.F.R. §164.308(a)(1)(ii)(A); 45 C.F.R. §164.306(a)(1)). Further, the example in the table above only measures an entity's compliance with specific HIPAA regulations; it does not identify and assess risks to the entity's ePHI. For example, for "Information Systems Activity Review" the table above only summarizes the entity's creation and implementation of policies and assigns a compliance rating - it does not identify and assess the risks to ePHI held by the entity for which activity review processes are ineffective or not in place.

For more information, please consult OCR resources for conducting a risk analysis (https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html) and OCR's HIPAA audit protocol for spotting gaps in compliance with the HIPAA Rules (See https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html).

**This newsletter should not be construed as a final agency action and is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter civil or criminal.*