WHITEPAPER

RISK ANALYSIS VERSUS RISK ASSESSMENT:

WHAT'S THE DIFFERENCE?

ANDREW HICKS
MBA, CISA, CCM, CRISC, HCISSP, HITRUST CSF PRACTITIONER
PRINCIPAL, HEALTHCARE AND LIFE SCIENCES

COALFIRE

North America | Latin America | Europe
877.224.8077 | info@coalfire.com | coalfire.com

TABLE OF CONTENTS

OVERVIEW

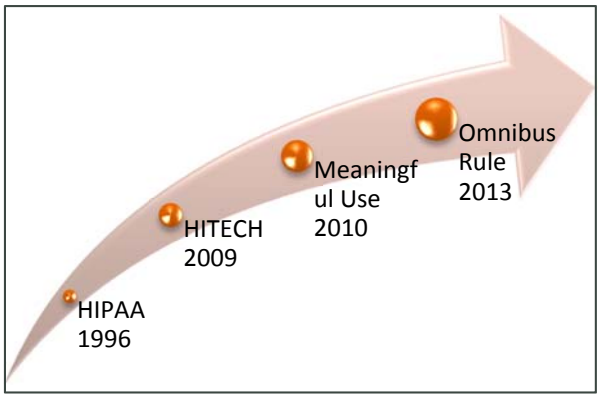
Risk analysis. Risk assessment. Compliance assessment. Are these concepts as confusing to you as they are for most IT professionals? Clearly, IT security experts are not in agreement as to whether these important concepts are synonyms, antonyms, or perhaps neither or both. Actually, the correct answer could differ based on a specific industry or regulation, even though they are not exclusive to either. The purpose of this paper is to shed some light on these often-misunderstood concepts. With a focus on the healthcare industry, we will dissect these concepts so that organizations not only walk away with a clear distinction, but also know what is *required* per the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

WHAT THE REGULATIONS SAY

The healthcare industry has seen a continuous release of regulations designed to modify or improve existing regulations. Consider the HIPAA Security Rule, the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Meaningful Use incentive program, and the recent Omnibus Rule. In all cases these regulations have continuously emphasized the importance for covered entities (CEs) and business associates (BAs) to assess and remediate risks to protected health information (PHI).

THE HIPAA SECURITY RULE

To comprehend the requirements for understanding risk, we must first start with what is required by HIPAA. The first requirement of the HIPAA Security Rule is a risk analysis (updated in 2013 by the Omnibus Rule). Per 164.308(a)(1)(ii)(A), a CE or BA must *"conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the covered entity or business associate."*



THE HITECH ACT AND OMNIBUS RULE

Until this point, we have seen no mention of the term "risk assessment." But wait! The release of the Interim Breach Notification Rule (now known as the Omnibus Final Rule) for the purpose of constituting a breach states that *"covered entities and business associates must assess the probability that the protected health information has been compromised based on a risk assessment."* Did you catch the substitution of analysis with assessment? Not only is this the first time that "risk assessment" has been used (outside of the public comments and responses in the federal register), but it is specific to assessing the risks in response to a suspected breach. Interesting.

Given these requirements, nowhere in any healthcare regulation is the concept of "risk assessment" as opposed to "risk analysis" differentiated. Let's continue by taking a closer look at some of the available guidance published by authoritative sources such as the Office for Civil Rights (OCR), the Centers for Medicare & Medicaid Services (CMS), and the National Institute of Standards and Technology (NIST).

MEANINGFUL USE

Moving through the healthcare regulatory timeline, the topic of risk is next addressed in the CMS requirements for satisfying Meaningful Use (MU), which is an incentive program for specific organizations that exhibit "meaningful use" of certified electronic health record (EHR) technology to improve patient care. Within the MU core objectives (stage 1 and 2), organizations are required to *"protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities."* To satisfy this objective, organizations are instructed to *"conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1),"* which is the risk analysis requirement defined above.

AUTHORITATIVE GUIDANCE

There are a few sources of guidance worth mentioning in this document. These are the sources that are highly regarded by IT security professionals in the healthcare industry and, in many cases, considered the de facto standards. The first is that of government/regulatory authorities such as the CMS, OCR, and Department of Health and Human Services (DHHS). Secondly, NIST, through its release of special publications, has been accepted by the industry and the OCR (mentioned in the Federal Register) as a comprehensive framework for achieving security and compliance. Let's take a closer look.

HIPAA SECURITY SERIES

With the enactment of the HIPAA Security Rule, the CMS, under the jurisdiction of the DHHS, developed the HIPAA Security Series as a way to give CEs insight into the Security Rule and provide assistance with the implementation of the security standards. Of the seven papers developed, the one directly related to this paper is number six, "Basics of Risk Analysis and Risk Management." Within this document, the CMS provides guidance on how organizations should evaluate the threats, vulnerabilities, and risk to ePHI, which forms the objective of the risk analysis requirement. However, in this particular case the CMS makes no differentiation between a risk analysis and a risk assessment and, in fact, only uses the word assessment once in an effort to identify sources of information to identify technical vulnerabilities.

NIST 800-66

While somewhat dated, NIST 800-66, formally known as *"An Introductory Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,"* was released in 2008 to help organizations understand the requirements of the Security Rule and to identify risk-mitigation controls that satisfy the requirements. Focusing on the risk analysis guidance of the publication, NIST uses both "analysis" and "assessment." However, in this case the term risk assessment is presented as an overarching concept to include both risk analysis and risk management – risk management being the second requirement (i.e., standard) within the Security Rule.

NIST 800-30

Updated in 2012, NIST 800-30 or the *"Guide for Conducting Risk Assessments"* is highly regarded among IT security professionals as the leading framework for performing risk assessments. The publication is not only referenced in NIST 800-66, but is continuously referenced in the HIPAA Security Series and among health IT subject matter experts. While the document does an excellent job of explaining the manner in which risk assessments should be performed, including the identification of threats, vulnerabilities

(containing impact and likelihood evaluation), risk, and control posture, an excellent piece of evidence in solving the confusion of risk analysis and risk assessment is found in the definition section. Per NIST, a risk assessment is defined as, *"The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis."* Did you catch that last sentence? According to NIST, risk assessment and risk analysis is one and the same. Furthermore, NIST 800-39 – *"Managing Information Security Risk Organization, Mission, and Information System View"* – upholds this definition.

SECURITY RISK ANALYSIS TIPSHEET

While the Security Risk Analysis Tipsheet is much lesser known, it's worth noting as it is the CMS' guidance for satisfying the MU core objective related to the protection of ePHI. In short, the CMS doesn't tell us anything we don't already know. In fact, it points directly to the HIPAA Security Rule risk analysis requirement to satisfy the objective. What's important however, is the fact that the CMS does not mention the concept of risk assessment within the five-page guide, but does provide guidance for satisfying the requirement that is similar to the process identified within NIST 800-30.

WEBSTER

Let's take a less sophisticated approach based on the assumption that analysis and assessment could be synonymous with each other. For this, we turn to our good friend, Merriam Webster. According to Webster, an analysis is *"a careful study of something to learn about its parts, what they do, and how they are related to each other,"* while assessment is defined as *"the act of making a judgment about something: the act of assessing something."*

CAUSE FOR CONFUSION

I think it's safe to say that a risk analysis and a risk assessment are synonymous with each other – at least in the eyes of the OCR, DHHS, CMS, authoritative sources, and the healthcare industry in general. While there appears to be no logical difference other than risk assessment relating more to how risks should be assessed through the breach notification process, the OCR (in both its guidance and formally within the Federal Register) appears to use the concepts interchangeably. Perhaps this is the source of the confusion. In fact, the HIPAA Security Rule Toolkit, which was developed by NIST in 2011 for the purpose of satisfying the risk analysis requirement, calls for the performance and documentation of a risk assessment. Furthermore, in a collaboration effort between the OCR and the Office of the National Coordinator for Health Information Technology (ONC), the Security Risk Assessment (SRA) tool was recently released. Within the user guide it states, *"Organizations may use the SRA Tool in coordination with other tools and processes to support HIPAA Security Rule – Risk Analysis compliance and risk management objectives."*

BEYOND THE CONFUSION: ASSESSING COMPLIANCE

The Security Rule, reinforced by HITECH and Omnibus, makes it clear that all organizations that create, receive, maintain, or transmit PHI are on the hook for compliance and the associated stiff penalties that may be enforced in the event of a security breach. This means that organizations need a formal risk management program (including risk analysis) and also an ongoing compliance evaluation program.

Under the evaluation requirement of the Security Rule, CEs and BAs are required to "Perform a periodic technical and nontechnical evaluation…in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart." In other words, an organization needs to perform continuous-monitoring assessments of its ePHI environment and implement controls to ensure that compliance with the Security Rule is maintained. These ongoing assessments should not only be policy- and procedure-based, but should also include the design and operating effectiveness of the manual and automated controls implemented to safeguard patient data.

Two common approaches to assessing HIPAA compliance are via gap and compliance assessments. While a gap assessment is designed to identify control gaps and control alignment with the regulations, it is primarily focused on control identification and design. On the other hand, a compliance assessment is designed to ensure that the ePHI control environment is operating effectively, that is each control is performing successfully and as designed. It goes without saying that a control gap, such as an unencrypted laptop, can result in a security breach, but a control that is not appropriately designed or not performing as intended, could also result in a breach. Therefore, both types of assessments are imperative to ensure HIPAA compliance is satisfied.

GAP ASSESSMENT	COMPLIANCE ASSESSMENT
Evaluates control design	Assesses operating effectiveness
Sample size of 1	Sample size based on frequency of control execution
Generally reserved for new systems/processes or organizations new to HIPAA compliance	Reserved for mature HIPAA programs
Lower level of effort (lower cost)	Higher level of effort (higher cost)
Basic understanding of ePHI assets	ePHI asset inventory required
Data flow diagrams recommended	Data flow diagram required

CONCLUSION

There are a couple things that are certain. First, the OCR is raising the bar in terms of compliance. Second, it's only a matter of time before unsecured data causes more breaches resulting in reputational damage and civil and monetary penalties. We also know that the OCR has consistently communicated concerns, guidance, and enforcement activities. As a result, the safety and privacy of patient information is of utmost concern and those organizations subject to the Rules must ensure that they are properly assessing their risks through a risk assessment/analysis process and managing their risks through the implementation of mature controls.

And with regards to the name game – risk analysis versus risk assessment – don't let your organization get wrapped up in semantics. Know what the regulations are and understand your responsibilities as an organization committed to securing patient and customer data.

RESOURCES

HIPAA Security Rule – http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/

HITECH – http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

CMS Meaningful Use – http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms/

HIPAA Omnibus Rule – http://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/

HIPAA Security Series – http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

NIST 800-66 – http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

NIST 800-30 – http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Security Risk Analysis Tipsheet – http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/SecurityRiskAssessment_FactSheet_Updated20131122.pdf

ABOUT COALFIRE

Coalfire is the global technology leader in cyber risk management and compliance services for private enterprises and government organizations. Our professionals are renowned for their technical expertise and unbiased assessments and recommendations. Coalfire's approach builds on successful, long-term relationships with clients to achieve multiple cyber risk management and compliance objectives, tied to a long-term strategy to prevent security breaches and data theft.

WP_RiskAnalysisVAssessement_050616