

ALL ABOUT THE HIPAA RISK ANALYSIS - from the OCR (HHS Office of Civil Rights)

Amazing Development. What a Great Surprise for a Risk Analysis/Risk Assessment Person! The Department of Health and Human Services, Office of Civil Rights finally came out with their draft guideline for the HIPAA Risk Analysis on May 10th!

While hospitals and health plans, business associates, technical service providers and physicians have struggled to understand the original HIPAA risk analysis requirement, the Health & Human Services Department finally published the draft guidance to help healthcare providers understand what is expected of them in doing a risk analysis of their protected patient health information (ePHI).

This is a critical part of the HIPAA Security Rule, but there was never any 'official' guidance of exactly what was expected and how they should accomplish the risk analysis.

Why the Office of Civil Rights? Because the new HITECH Act (February 2010) directed that OCR oversee health information privacy including the enforcement of the HIPAA requirement. And the guidance is long overdue. I have had dozens of conversations with individuals at hospital and healthplans, discussing what a risk analysis is, what are the basic elements, and I am THRILLED to report that the OCR agrees with my methodology.

The draft guideline on risk analysis also takes the same track that the financial institutions have given as guidance to banks and credit unions. That is risk analysis is a foundational document that should be used (and referenced) as the organization evaluates and implements appropriate controls.

OCR refers to the risk analysis, not as a one-time drill, but instead, as an ongoing process to help organizations evaluate their risk focusing on the confidentiality, integrity and availability of protected health information. The Risk Analysis Report, creates the blueprint that an organization will follow as they improve their compliance – for example, deciding what data should be authenticated in particular situations, deciding, when, if or how to use data.

A risk analysis is also the basis for an understanding by organizations of the technologies they will need to secure protected health information, OCR said in the draft guidance May 7.

To quote directly: “*We begin the series with the risk analysis requirement in § 164.308(a)(1)(ii)(A). Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule.*”

Therefore, a risk analysis is foundational, and must be understood in detail before OCR can issue meaningful guidance that specifically addresses safeguards and technologies that will best protect electronic health information.”

Among the basic elements of a risk analysis, OCR said, organizations must identify data collections, document threats to information that could create a potential for inappropriate disclosure and assess current security measures the organization uses to protect patient information. This was great to read because it follows the elements I have built our solutions around.

Those elements, which were reinforced by the draft guideline include the following five elements of risk analysis (and risk assessment).

1. Identify and characterize the assets that need protection, including the databases, the applications, etc.
2. Analyzing the relevant threat data – focusing on what could adversely affect the assets (ePHI) in this case.
3. Modeling the potential losses that could result from the threat actually materializing.
4. Finding the existing vulnerabilities in the current security situation that would increase the odds of the loss actually occurring.
5. Developing appropriate controls to reduce potential loss, reduce existing vulnerabilities and make sure the controls are cost effective.

The OCR also referenced the NIST 800-66 to show sample questions that need to be part of the risk analysis. Luckily – we totally agree with them and have included the NIST 800-66 Guidance in every HIPAA Risk Analysis Solution.

Here’s another short excerpt from the OCR:

“Risk Analysis Requirements under the Security Rule

The Security Management Process standard in the Security Rule requires organizations to “[i]mplement policies and procedures to prevent, detect, contain, and correct security violations.” (45 C.F.R. § 164.308(a)(1).)

Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard. Section 164.308(a)(1)(ii)(A) states:

RISK ANALYSIS (Required).

Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization].

OCR went on to cite NIST 800-66: *“The following questions adapted from NIST Special Publication (SP) 800-66 are examples organizations could consider as part of a risk analysis. These sample questions are not prescriptive and merely identify issues an organization may wish to consider in implementing the Security Rule:*

- Have you identified the e-PHI within your organization? This includes e-PHI that you create, receive, maintain or transmit.*
- What are the external sources of e-PHI?*

The publication of this first draft guideline gives healthcare organizations and other affected organizations a hint about which direction the OCR enforcement is going to go. As I mentioned previously, the regulators are likely to follow the example of financial audits and ask for the current copy of the organization’s risk analysis and use that as the blueprint to measure how well the organization used the risk analysis to prescribe and dictate all other actions which were taken to protect the organization’s protected health information.

In the words of the OCR – ***“In Summary, Risk analysis is the first step in an organization’s Security Rule compliance efforts. Risk analysis is an ongoing process that should provide the organization with a detailed understanding of the risks to the confidentiality, integrity, and availability of e-PHI.***

For a complete copy of the 8 page OCR guideline, please send an email to info@riskwatch.com.