
E-BRIEF SERIES
Healthicity
6 Reasons You Should Outsource Your Risk Analysis

Risk Analysis is the Cornerstone of All of Your Information Security Activities

Summary

Risk analysis is the cornerstone of your information security activities. Taking it seriously is crucial for maintaining compliance and protecting your organization's reputation.

Introduction

Risk analysis is the cornerstone of all of your information security activities. For example, Meaningful Use is a critical initiative for healthcare organizations and risk analysis is requirement #1 (Protect ePHI) for the modified stage 2 criteria. Not taking it seriously can be dangerous to your organization's reputation.

Due to its importance, there are a number of reasons most organizations should choose to outsource. Most organizations simply don't have the resources or the expertise to conduct their own, adequate, risk analysis.

6 GOOD REASONS YOUR ORGANIZATION SHOULD OUTSOURCE ITS RISK ANALYSIS

1

MOST ORGANIZATIONS DON'T HAVE THE RESOURCES OR THE EXPERTISE TO CONDUCT A RISK ANALYSIS.

The rules don't necessarily require third-party risk analysis. Covered entities and business associates are free to conduct their own. But, for the same reasons organizations hire lawyers, accountants, and engineers, most organizations are better off hiring an outside firm. Most organizations don't have the resources or the expertise for the methodical processes necessary for conducting a risk analysis. Even the use of self-assessment tools, such as the one provided by the ONC, are problematic because these tools are often poorly designed. For example, they may facilitate the creation of an inventory but completely separate the inventory from the assessment of risks. Often, using these tools requires expertise that organizations don't have. So you may end up with a report that is stamped, "Risk Analysis," but the results are often inadequate.

2

AN INADEQUATE RISK ANALYSIS IS JUST AS DANGEROUS AS A MISSING RISK ANALYSIS.

The recent resolution agreement with Advocate Health Care Network makes it clear, that in addition to simply conducting risk analysis, organizations need to conduct one that meets the regulation requirements to document ALL risks and threats to ePHI. Advocate had a risk analysis on record, but that risk analysis had many holes in its scope and process. The corrective action plan required Advocate to revise its risk analysis to include:

"All Advocate facilities, whether owned or rented, and evaluate the risks to the ePHI on all of its electronic equipment, data systems, and applications controlled, administered or owned by Advocate or any Advocate Entity, that contain, store, transmit, or receive ePHI… a complete inventory of all of its facilities, electronic equipment, data systems, and applications that contain or store ePHI…"

Does your risk analysis do this?

3

MEANINGFUL USE IS A CRITICAL INITIATIVE FOR HEALTHCARE ORGANIZATIONS AND FOR THE MODIFIED STAGE 2 CRITERIA, THE RISK ANALYSIS REQUIREMENT (PROTECT EPHI) IS #1.

For eligible providers, the risk analysis requirement was #15 for MU stage one, and #9 for MU stage two. But, for modified stage 2 and stage 3, it's requirement #1. Modified stage 2 will be the required criteria from 2015 to the end of 2017, when stage 3 requirements will take effect and be incorporated into MIPS. We know from our FOIA request in 2014 that, as of then, about 25% of eligible providers failed their meaningful use audit (repost and link to infographic). And we know from modified stage 2 rulemaking that they failed because of missing or inadequate risk analysis. Administrators also it made clear that the risk analysis requirement will continue into MU stage 3 in 2018.

4

RISK ANALYSIS IS THE CORNERSTONE OF ALL YOUR INFORMATION SECURITY ACTIVITIES.

The risk analysis is the HIPAA requirement that bolsters all your information security activities. It provides the basis for decision-making, for what controls need to be put into place. And what your budget should be for information security. It's the rule that requires you to know, to know what your risks are, which information security controls are working, which ones are failing and which ones are missing.

It's a methodical, comprehensive and rigorous process to fully understand potential risks and to document them efficiently. And to provide the information to mitigate those risks to a reasonable and appropriate level. Ignorance is not allowed nor is it an excuse. Risk analysis determines and documents potential problems or risks to ePHI in your organization. If you don't conduct a comprehensive risk analysis, THEN YOU ARE JUST GUESSING AND HOPING.

5

RISK ANALYSIS AND RISK MANAGEMENT REQUIRE ACTIVITIES AND CONTROLS FOR INFORMATION SECURITY THAT ARE NOT EXPLICIT IN THE REGULATIONS.

There are certain information security controls that are explicit in the regulations. All users must have their own username and password §164.312(a)(2)(i). Entities must have defined processes for auditing and monitoring access to systems (§164.308(a)(1)(ii)(D)) and a data backup plan in place (§164.308(a)(7)(ii)(A)).

But regulators and the OCR are able to require covered entities to take actions and implement controls that are not explicit in the regulation and risk analysis is one of the two big "gray areas" of HIPAA compliance (the other being addressable safeguards). Multiple guidance documents and resolution agreements make it clear that it's the responsibility of organizations to take necessary steps to protect ePHI, the first step being risk analysis, which also happens to be the most important tool for organizations to understand how to implement the regulations in a practical way. The regulations require authentication mechanisms (§ 164.312(c)(2) but what authentication mechanisms should you put in place? Complex password managed through Active Directory Group Policies? Or two-factor authentication with single sign-on? Your risk analysis will help you decide. What should the recovery time objective (RTO) be for your data backup plan? Unsurprisingly, you can lean on your risk analysis for that too.

6

THIRD-PARTY RISK ANALYSES ARE SEEN AS MORE OBJECTIVE AND CREDIBLE BY REGULATORS.

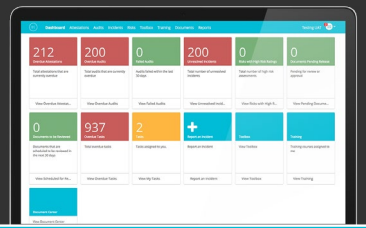
We regularly meet with regulators, experts and auditors. And it seems that without fail, a third-party assessment is seen as more credible and objective from their perspective. Self-assessments suffer from the "fox guarding the hen-house" syndrome where assessors are unable or unwilling to take the steps necessary to comply with the risk analysis requirement even if they have the expertise to conduct one. Self-assessments can run into conflicts of interest as a quality risk analysis may reveal issues that implicate the assessor or the assessor's friends. In other words, the risk analysis may reveal problems that IT personnel should have known about. Lastly, self-assessments can suffer from the curse of the familiar. Staff conducting a risk analysis can become blind or inured to problems because they are constantly right in front of us. The "fresh eyes" of a third-party assessor can overcome this problem.

Conclusion

Risk analysis is the cornerstone of your information security activities and an important requirement for meeting meaningful use. While it is an option for your organization to attempt to conduct a Risk Analysis on your own, your compliance are reputation are safer in the hands of an expert. We recently launched our own Risk Manager, designed by our compliance experts, with your specific needs in mind. By addressing all areas of HIPAA privacy and security requirements, including Administrative Safeguards, Technical Safeguards and Physical Safeguards (or ATP), you can rest assured knowing that your results will be comprehensive.

For more on Healthicity's Compliance Services and Solutions, please visit healthicity.com/compliance or call 877.777.3001

Risk Assessment Manager



WATCH ON-DEMAND DEMO

Resource Center

EXPLORE FREE RESOURCES