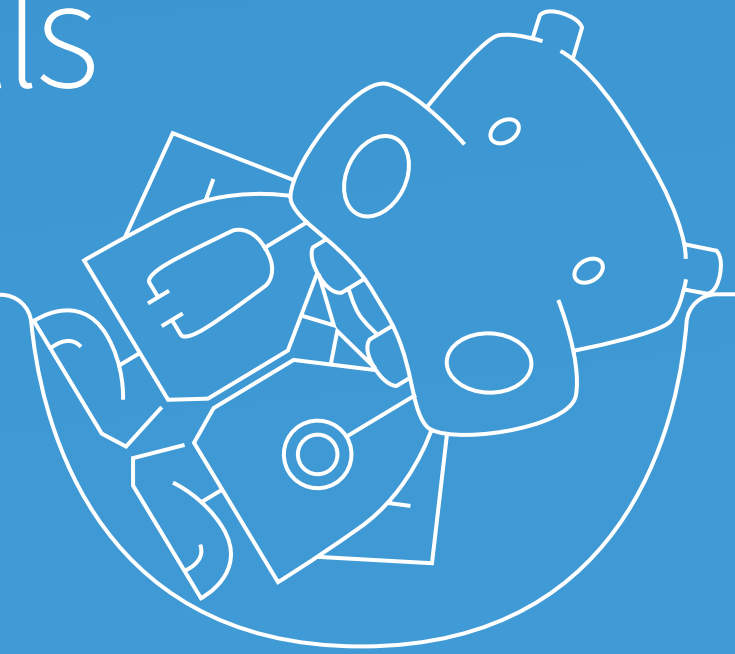
HIPAA Risk Analysis & Risk Management Program Considerations: Common Pitfalls



schellman
Quality. above all.

WHITEPAPER

Because **more than 90% of OCR enforcement actions call out failure with Providers' HIPAA Risk Analysis & Risk Management processes,** it seems to make sense to place special concentration on these specific HIPAA requirements.

Having performed full HIPAA assessments for over 15 years and now having introduced our HIPAA Express service that focuses on that specific section of the rules, we're going to provide some insight to make that special concentration possible.

In this article, we'll do a deep dive into the risk requirements and highlight general problems often found in risk analysis/risk management activities so that you can avoid them. Don't be among that 90%–read on to help ensure HIPAA compliance.

What are the HIPAA Risk Requirements?

The applicable HIPAA requirements are listed below:

Requirement	Details
§164.308(a)(1)(ii)(A) **(Risk Analysis)**	**Definition:** *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 covered entity or business associate.* **What It Means:** You must perform risk analysis (as this is the first step to management).
§164.308(a)(1)(ii)(B) **(Risk Management)**	**Definition:** *Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).* **What It Means:** You should make informed decisions based on the results of the risk analysis required in §164.308(a)(1)(ii)(A) to reduce your risk.
§164.306(a)	**Definition:** *Covered entities and business associates must do the following:(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part; and (4) Ensure compliance with this subpart by its workforce.* **What It Means:** The Risk Management requirement asks that you reduce risk—now this very broad statement essentially says that risks and vulnerabilities must be reduced to a reasonable and appropriate level for all the requirements in the HIPAA Security Rule.

Common Pitfalls in HIPAA Risk Analysis/Risk Management

As this language isn't prescriptive, it often causes confusion—hence the aforementioned 90%.

The fact is, doing a high-level risk assessment isn't enough. And though many organizations may believe that's the case, they often fall victim to three common problems:

1. SCOPE IS TOO SMALL

In many of its breach investigations, the OCR found that the scope of systems covered in an organization's risk analysis/management program failed to consider all places ePHI could be located in their environment.

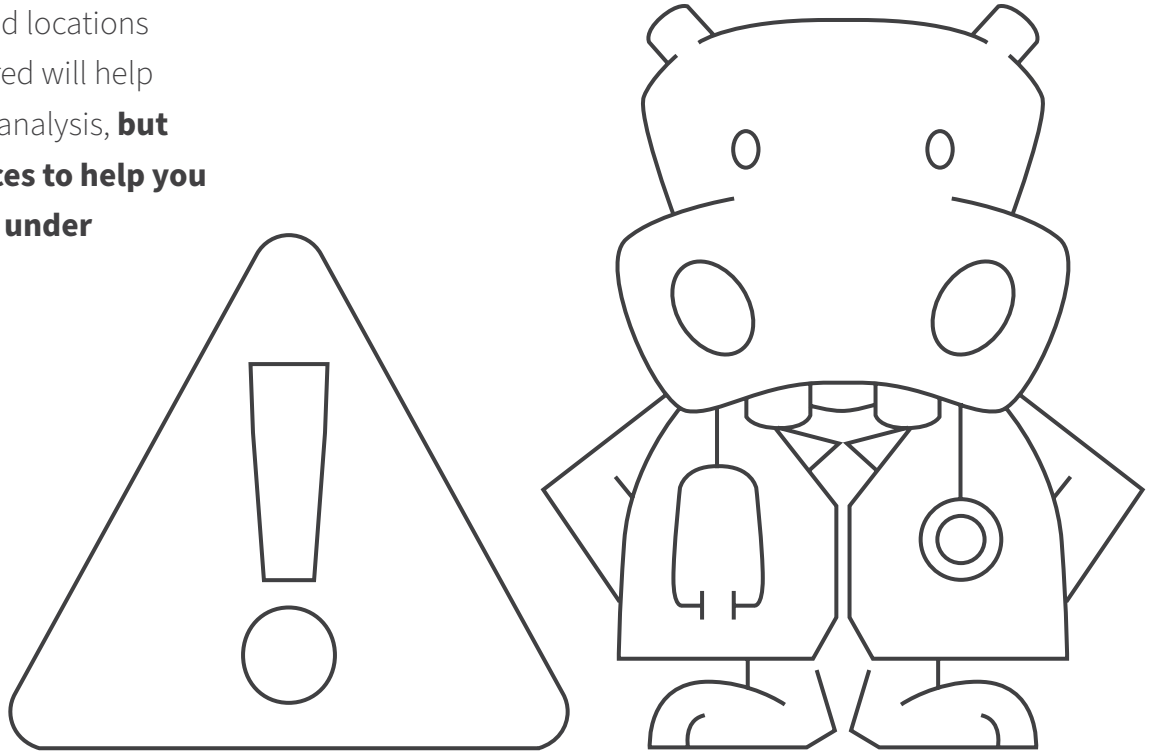
The penalties for violations are so severe that it's better to be safe than sorry—if you're handling ePHI as part of your services provided, and you don't know for sure which systems the ePHI is restricted to, you should assume that all systems in the environment are in scope for HIPAA.

But at the end of the day, it's very difficult to implement an effective risk analysis/risk management program without truly knowing how ePHI flows through your environment or what systems are involved. **As such, identifying ePHI and the various pieces that it touches will be your necessary first step in developing a HIPAA-compliant risk analysis/risk management program—we recommend first segmenting out systems that could receive, transmit, or store ePHI.**

Common Pitfalls in HIPAA Risk Analysis/Risk Management (cont.)

2. INADEQUATE RISK ANALYSIS

Figuring out the in-scope systems and locations where ePHI is stored or could be stored will help ensure you perform satisfactory risk analysis, **but there are also some great resources to help you build your program that often fly under the radar:**



Resources

OCR Guidance on the Risk Analysis Requirement

- The OCR guidance is not an exact template for performing a risk analysis, but what it does do is clarify OCR expectations in terms of high-level steps that should at least be part of the process, including 9 essential elements to a quality risk analysis.
- Given that the OCR is the organization that investigates breaches, incorporating their guidelines is something to consider.

NIST SP 800-30

—the Guide for Conducting Risk Assessments

- The aforementioned OCR Guidance makes multiple references to this publication. While you don't have to follow its risk assessment methodology exactly, it is a well-known and established methodology, and clearly the OCR values it as a guide.

Security Risk Assessment Tool

- Developed in collaboration with the OCR by the Office of the National Coordinator for Health Information Technology (ONC), the nice thing about this tool is that it not only guides the risk analysis process but also pulls in the actual requirements in the HIPAA Security Rule.
- You'll be able to not only identify where you might not be meeting these requirements, but the tool will also provide some items for compliance consideration, including example threats, vulnerabilities, and potential safeguards for each requirement. You'll also have a place to identify if a risk for each specific requirement is high/medium/low for likelihood, impact, and overall risk.

Having a robust risk analysis using the information in these tools can help you for the next step, which is compliance with §164.308(a)(1)(ii)(B)—or control implementation to reduce the risks to a level that is "reasonable and appropriate" to comply with the HIPAA Security Rule requirements.

Common Pitfalls in HIPAA Risk Analysis/Risk Management (cont.)

3. LACK OF FORMAL REASSESSMENT

But after all that, there's another area among the requirements that a lot of organizations overlook:

164.316(b)(2)(iii) Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

Common Pitfalls in HIPAA Risk Analysis/Risk Management (cont.)

As we've laid out, you should complete great risk analysis and then implement controls that address the identified risks to a "reasonable and appropriate" level, but you can't just then forget about it. **You must have:**

- A formal process to reassess risk on a specified basis, as well as
- A process to perform an updated analysis when new substantial risks are identified due to a major change in your environment.
    - Examples of such new areas of risk include new technologies introduced or new business operations that are implemented.

We've seen the OCR issue multiple fines to organizations that failed to incorporate new risks into their risk program, making it clear that these aforementioned processes are expected and necessary to comply with HIPAA.

Ideally, you should do an annual reassessment, but your best case scenario would be making an integrated risk analysis and management process part of your new technology or business operations planning.

Avoid Non-Compliance with HIPAA Risk Analysis/Risk Management Requirements

Aside from these tips and different guidance, **there's another way you can help yourself avoid non-compliance with HIPAA risk requirements—you can undergo Schellman's HIPAA Express assessment.**

Designed specifically for healthcare providers and systems, this new service offering of ours addresses HIPAA risk analysis and management specifically to help organizations avoid falling victim to the OCR's particular emphasis on these requirements. Because it is specifically focused, it's a scaled-down assessment, which means less burden on your budget and a shortened timeline.

And **you receive a report that will help demonstrate your due diligence in this highly important area of HIPAA compliance, with information on your security and risk profile, which could really help in the event of an OCR investigation.** To learn more about how this service can serve you, please contact us.

Next Steps for HIPAA Compliance

The importance of these HIPAA risk analysis/risk management requirements cannot be overstated. It's very easy to fall into common shortcomings when establishing compliance, and so you should prioritize these risk requirements—not just so you preserve your compliance with HIPAA, but also possibly avoid being fined for a breach.

But now you have some extra information that will help inform your approach including a brand new assessment option, should you so choose. **As you consider the guidance tools out there and begin to strengthen your reassessment protocols, read our other articles that can both help you avoid violations and provide an incentive to do so:**

- HIPAA Violations and How to Avoid Them
- HIPAA Violations & Penalties: Civil vs. Criminal

CLICK FOR MORE INFO

www.schellman.com
4010 W Boy Scout Blvd, Suite 600 / Tampa, FL 33607 / 1.866.254.0000
Outside of the United States, please dial: +1.813.288.8833