Risky Business: How to Conduct a Bona Fide HIPAA Security Risk Analysis

By Bob Chaput, CISSP, CIPP/US
Founder, Clearwater Compliance LLC
Risky Business

Many organizations have ignored the HIPAA Security Rule over the past several years, while others have just fallen behind in their compliance efforts. And some aren’t even aware of their obligations under the law. For those who aren’t prepared, the future holds stiff penalties that will adversely impact bottom lines and organizational brands.

Risk analysis is a core foundational step toward HIPAA compliance, yet organizations largely have been found lacking in this area. In 2012, 68 percent of Covered Entities and 80 percent of Providers had adverse Risk Analysis findings when audited by the Office for Civil Rights. Since 2008, 100 percent of settled cases from OCR investigations cited bona fide Security Risk Analysis as a corrective action plan requirement.

With a rising number of complaints, high-profile breaches and sub-par performance by audited organizations, OCR is lowering the boom on organizations failing to complete the foundational Risk Analysis requirement in the HIPAA Security Rule. As a result, it's time to get ready.

This whitepaper is intended to provide helpful information on how to perform a bona fide security risk analysis that meets both the requirements of the HIPAA Security Rule and Meaningful Use. Specifically, it will cover:

- Bona Fide Security Risk Analysis Essentials
- Specific Requirements Outlined in HHS/OCR Final Guidance
- A Practical Risk Analysis Methodology
- Step-by-Step Instructions for Completing a HIPAA Security Risk Analysis
- Best Practices from Leading Organizations
- Tools, Templates and Forms Available to Help
Why Risk Analysis?

The stakes have been raised. Organizations can no longer hide behind “not being aware” of risks to avoid penalties. Nor can they expect a slap on the wrist when penalties are issued.

As HHS Office for Civil Rights Director Leon Rodriguez recently stated, the final Omnibus rule not only greatly enhances patient rights and protections but also “strengthens the ability of my office to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates.”

Rodriguez has consistently stated that his office will aggressively pursue penalties for organizations that show “an ongoing failure to comply with HIPAA Privacy and Security Rules” citing a missing or insufficient risk analysis as a common failure. Such organizations will likely be subject to “willful neglect” penalties, which carry a minimum of $50,000 per patient/per day for each violation cited. Basically, willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the regulations.

This is the brave new world. If your organization is rolling the dice, you are placing your business at significant risk.

It’s not just about the audit.

Conducting a bona fide risk analysis isn’t just an insurance policy you take out in case your organization is randomly selected for an OCR audit. In fact, odds are you’ll never be among the chosen few who go through the audit process. The bigger reason for making sure you adhere to the guidelines and thoroughly analyze you risks is to avoid formal investigations. An even bigger reason is to maintain the trust and confidence your patients, members or customers have in your organization.

Many activities can trigger an OCR investigation, including:

Complaints – More than 1,000 consumer complaints are filed with OCR each month. That number will grow as individuals receive additional incentives to report violations.

Breaches – Once you report a breach of PHI, you will get a long, hard look from OCR. Failure to show an appropriate risk analysis will quickly escalate the severity of your situation.

State-Level Inquiries – The State Attorney General’s office as well as other state organizations (i.e. California Department of Public Health) can spark an OCR investigation.

Risk analysis is even more important in the context of HIPAA compliance than ever. If you are a covered entity, you are now also responsible for how well your business associates comply with the law, specifically how well they have assessed potential risks. What’s more, if you are an organization seeking meaningful use incentive monies, you must certify that you’ve conducted a risk assessment and started addressing your weaknesses.

If done the right way, a risk analysis can have you prepared for a successful audit experience. It can have you better equipped to respond to an OCR investigation, or even to avoid an investigation altogether. A proper risk analysis is the foundation of your security efforts and offers a platform for effectively conducting risk management activities in a way that will protect your organization and the personal health information of the people you serve.
What is a Risk Analysis?

The state of healthcare information risk analysis and management is a mess. There are no standards in terms of tools, approaches or even terminology. Amidst the confusion and inconsistency, many organizations are simply not doing it the right way.

More than 627 organizations in the United States have reported breaches of 500 or more patient records. More than 22 million Americans have been affected by these lapses in security. As we stated earlier, whenever organizations come under scrutiny by way of audit or investigation, they almost always are found lacking in the area of risk analysis.

This begs the question: what constitutes a bona fide risk analysis?

Let’s first answer the question by stating what a risk analysis is NOT. The following is a list of important activities that are sometimes thought of as “good enough” for analyzing risk.

- Network vulnerability scans
- Penetration tests
- Social engineering tests
- Configuration audits
- Network diagram reviews
- Questionnaires
- Information system activity reviews
- Security evaluation

Again, while each of these activities has value and an important role to play, none of them will hold up when compared to the requirements and expectations under HIPAA-HITECH for conducting a risk analysis. The last entry on the above list, security evaluation, is an important one to highlight. Many organizations mistake this as being one in the same as a risk analysis, when in fact it is not. A security evaluation only establishes the extent to which an entity’s security policies and procedures meet requirements. A risk analysis is much more.

As stated in the NIST Special Publication SP800-30, a risk analysis is the process of identifying, prioritizing and estimating risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, 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.
Defining Risk

In order to fulfill the requirements stated above and to successfully execute a risk analysis process, you need to have a solid understanding of key terminology and what constitutes real “risk” in the first place.

Here are a few important terms that need to be clearly defined.

**Asset** – any property, system or object that stores, shares or otherwise accesses protected health information (i.e. laptop, server, etc.)

**Threat** – the potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

**Vulnerability** – 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.

**Controls** – actions taken to reduce the likelihood of an undesired event

And then we must define the most important term: **risk**.

Risk is a derived value (like speed, which is calculated by distance/time). It is measured by the probability or likelihood an issue will occur, as well as the severity of the impact that issue would have. In order for risk to be present, you must have an asset, a threat AND a vulnerability present in the scenario. If one of these three variables is missing, there is no risk. For instance, a laptop (which is an asset) that is not encrypted (which is a vulnerability) but is locked away in a secure building and not connected to the internet is not a risk because there is no threat present.

Once you’ve established the presence of risk (asset x threat x vulnerability) and have assessed the likelihood of the threat exploiting the vulnerability and, were it to do so, the impact or harm, you must determine how to respond that risk. There are typically four paths. You can accept it, transfer it, mitigate it or avoid it. Your response is dictated by the likelihood of an adverse event occurring, coupled with the potential impact it would have.

If you (and/or any vendor you hire to support your compliance efforts) aren’t frequently using the terminology outlined above and addressing risks in terms of likelihood and impact, you need to rethink your approach. And fast.
Do your homework. Spend time with HHS/OCR guidance to make sure you have a full understanding of risk analysis requirements. Carefully select an outside partner to assist you in getting and staying compliant.

Update your risk analysis periodically. Thoughtful and effective risk analysis activities should occur at least annually, and should also be triggered whenever there is significant change within the organization.

Ensure your approach is consistent and repeatable. Assign a point person to coordinate risk analysis activities. Use common terminology and processes across your enterprise. Use a standard format and methodology across regions/facilities.

Have a system in place for managing risk. Make sure you have effective tools to help you identify and manage your risks. This system should also assist in the management and documentation of your ongoing risk analysis and management activities. Excel spreadsheets or other manual processes will likely come up short. The complexity of risk analysis and management requires sophisticated software and systems.

Set realistic goals. When addressing your vulnerabilities, make sure your goals are achievable. OCR will be fair, if you have a plan. Additionally, be diligent in rating your risks so you can prioritize based on severity. You won’t be able to tackle everything at once.

Examine your vendors. If you turn over any important operation to an outside partner or associate, you now are responsible for making sure they are doing everything they can to protect information as well. The government will expect that you have appropriately researched and vetted your vendors.
In Summary

How would you fare in an OCR audit or investigation? The financial, legal, regulatory and reputational consequences of not conducting a formal risk analysis and taking steps to mitigate identified risks are dire! At end of the day, what you’re seeking is ASSURANCE THAT:

- Your risk analysis scope includes all information assets used to create, receive, maintain or transmit ePHI
- All your risk analysis reporting facilitates better, more informed risk treatment decisions
- Your storage media used to create, receive, maintain or transmit ePHI is analyzed
- All reasonable and appropriate administrative, physical and technical controls are considered
- All relevant threat sources and threat agents are considered
- All relevant vulnerabilities are identified and considered
- Your risk analysis serves to identify, value and prioritize ALL risks
- You have fast, easy, anytime, anywhere access to your risk management profile
- Your business risk management goals are being met
- Your risk analysis specifically addresses the elements a risk analysis must incorporate as outlined in the HHS/OCR Guidance on Risk Analysis Requirements under the HIPAA Security Rule
- Your risk analysis meets the requirements set out in the OCR Audit Protocol on Risk Analysis

Your information is more valuable AND vulnerable than ever. As a result, the focus on risk analysis will continue to grow. We predict that risk analysis will remain one of the top three priorities for OCR as they audit and investigate HIPAA compliance, and that organizations that fail to show good faith effort in this area will be consistently and substantially penalized.

Is your organization ready, or are you at risk?
Resources

The following is a list of key resources to help you further understand the specifics of HIPAA risk analysis and to set your process in motion. We highly encourage you to spend time with each of these tools.

**ONC Guide to Privacy and Security of Health Information**

**HHS / OCR “Guidance on Risk Analysis Requirements under the HIPAA Security Rule”**
OCR Audit Program Protocol

**HIPAA Risk Analysis Buyers Guide**

**Webinar: How To Conduct a Bona Fide HIPAA Security Risk Analysis**

More Information?

Have questions regarding this whitepaper? Want to engage with us for a specific discussion about your risk analysis approach? You can share a note with any of our authors by reaching out: info@clearwatercompliance.com

About the Author

Bob Chaput is CEO and Founder of Clearwater Compliance LLC. His 30-year career includes 25 years in regulated industries, with 20 of those years spanning the highly security- and privacy-regulated healthcare industry. Over the course of his career, Chaput has been responsible for ensuring the privacy and security of some of the world’s largest healthcare databases, including senior executive roles at GE, Johnson & Johnson and Healthways, Inc.

He has also built, grown and sold a number of businesses serving industries with strict regulatory requirements, with deep experience in HIPAA and HITECH rules. He speaks and writes extensively on HIPAA and HITECH privacy, security and breach notification matters and is a recognized HIPAA-HITECH compliance expert. Chaput holds undergraduate and graduate degrees in mathematics, numerous technical certifications and is a Certified Information Systems Security Professional (CISSP), Certified Information Privacy Professional (CIPP/US), Certified HIPAA Professional (CHP) and a Certified HIPAA Security Specialist (CHSS).

About Clearwater Compliance

Clearwater Compliance, LLC, is all about and only about helping healthcare organizations and their service providers become and remain HIPAA-HITECH Compliant. Owned and operated by veteran, C-suite health care executives, Clearwater Compliance provides comprehensive, by-the-regs software and tools, risk management solutions, training, and professional services for small medical practices and healthcare startups to major healthcare systems, health plans and Fortune 100 companies. Since 2003, the company has served more than 350 organizations (including 100 hospitals). Find out more at clearwatercompliance.com.

© 2014 Clearwater Compliance LLP. This article is intended for general information purposes only and should not be construed as legal advice or legal opinions on any specific facts or circumstances.