Risky Business: How to Conduct a NIST-based Risk Assessment to Comply with HIPAA and Other Regulations

By Bob Chaput, MA, CISSP, HCISPP, CRISC, CIPP/US
Founder & CEO Clearwater Compliance LLC
In addition to being a regulatory requirement, conducting regular risk analyses is a fundamental business practice, yet organizations largely have been found lacking in this area.

“Risk comes from not knowing what you’re doing”
Warren Buffet

Risky Business

Despite the many warnings from the Office for Civil Rights (“OCR”) of the weaknesses uncovered during the 2012 HIPAA compliance audits, many organizations have continued to ignored the HIPAA Security Rule requirement to conduct periodic risk assessments.

Of the 25 Settlement Agreements between non-compliant organizations and OCR since 2008, 18 (72%) had not conducted a bona fide risk analysis, and some of these are big organizations (e.g. Columbia University, NY Presbyterian Hospital, WellPoint, BCBS of Tennessee, UCLA just to name a few). At an American Bar Association conference in June 2015, OCR Director Jocelyn Samuels described OCR’s investigative process which begins with a request for a documented risk analysis and risk management plan, in addition to evidence of risk management plan implementation. And estimates for the return of meaningful use “(MU)” incentive monies due to the lack, or insufficient conduct, of a bona fide risk analysis are north of $30 million according to Health Security Solutions.

In addition to being a regulatory requirement for PCI, HIPAA and MU, among others, conducting regular risk analyses is fundamentally good business practice, yet organizations largely have been found lacking in this area.

Risk is like fire: If controlled, it will help you; if uncontrolled, it will rise up and destroy you.”
Theodor Roosevelt

It’s time to get ready!

This whitepaper is intended to provide helpful information on how to perform a bona fide NIST-based security risk analysis as recommended by OCR, HHS and PCI DSS. Specifically, it will cover:

• Bona Fide Security Risk Analysis Essentials
• Specific Requirements Outlined in HHS/OCR/PCI-DSS
• 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 former HHS Office for Civil Rights Director Leon Rodriguez 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 OCR 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 1,400 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 state or federal investigations.

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. Many organizations are simply not doing it the right way, confusing risk analysis with security assessments.

More than 1,250 organizations in the United States have reported breaches of 500 or more patient records. More than 135 million records have been impermissibly disclosed or stolen by these lapses in security. As we stated earlier, whenever organizations come under scrutiny by way of audit or investigation, they are almost always found lacking in the conduct of a bona fide 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

“If you do not change direction, you may end up where you are heading.”
Lao Tzu
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 creates, receives, maintains, transmits or otherwise accesses protected health information or other sensitive data (i.e. laptop, server, backup tapes, mobile devices, etc.)

**Threat** – the potential for a person or event 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 that could occur if a threat exploits a vulnerability. And then we must define the most important term: **Risk**.

**Risk** – a derived value (like speed, which is calculated by distance/time). It is measured by the probability or likelihood an event will occur, as well as the severity of the impact that event would have. In order for risk to exist, 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 with sensitive information (the asset) that is not encrypted (the vulnerability) but is locked away in a secure building and not connected to the internet would not constitute a risk if indeed there are no threats present.

**Risk Register** – a rank ordered listing of all the risks identified during the risk analysis process.

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 classically four risk response choices.

You can accept it, transfer it, mitigate it or avoid it. Your response is dictated by the level of likelihood of an adverse event occurring, coupled with the level of potential impact it would have.

If you (and/or any vendor you hire to support your risk analysis efforts) are not using the terminology outlined above to address 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? Are your safeguards reasonable and effective enough to prevent a breach? The financial, legal, regulatory and reputational consequences of not conducting a formal risk analysis and taking steps to mitigate identified risks are dire! At the 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
- All information assets and media used to create, receive, maintain or transmit ePHI are 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 the top priority 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?

Your information is more valuable AND vulnerable than ever. As a result, the focus on risk analysis will continue to grow.
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

NIST Guide for Conducting Risk Assessments

HHS / OCR “Guidance on Risk Analysis Requirements under the HIPAA Security Rule”

2012 OCR Audit Program Protocol

HHS Risk Analysis Buyers Guide

HHS Security Risk Assessment Tool for Providers in Small and Medium Sized Offices

Webinar: NIST-Based Security Risk Analysis and Risk Management

To learn more about our risk analysis solutions, visit: https://clearwatercompliance.com/hipaa-solutions/hipaa-compliance-software/

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 Authors

Bob Chaput is CEO and Founder of Clearwater Compliance LLC. His 35-year career includes 30 years in regulated industries, with 25 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, focuses on helping healthcare organizations and their service providers improve patient safety and the quality of care by assisting them to establish, operationalize and mature their information risk management programs. Led by veteran, C-suite healthcare executives, Clearwater provides comprehensive, by-the-regs software and tools, educational events, and expert professional/advisory services for healthcare organizations ranging from major healthcare systems, hospitals, health plans and Fortune 100 companies, to medical practices and healthcare startups. Since 2003, the company has served over 450 organizations. Find out more about our privacy, security, compliance and information risk management solutions at clearwatercompliance.com.

© 2015 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.

1 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/