Guide

# Nine Network Considerations in the New HIPAA Landscape

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Omnibus Final Rule, released January 2013, introduced some significant changes and updates. The HIPAA Omnibus Final Rule may change how you conduct business. At the same time, the 2012 audits concluded with some initial findings. The HIPAA Audit Results from the pilot of 115 audits may impact how you run your internal organization and network.

Given these latest changes, it's imperative that you understand the impact this may have on your IT group and your network. Here are nine things to consider about how the HIPAA Omnibus Final Rule and 2012 HIPAA audit results could impact your IT network and IT processes.

1. HIPAA Audits will continue
2. The HIPAA Audit Protocol and NIST 800-66 are your best preparation
3. Knowledge is a powerful weapon – know where your PHI is
4. Risk Assessment drives your baseline
5. Risk Management is continuous
6. Security best practices are essential
7. Ignorance is not bliss
8. Your business associate(s)must be tracked
9. Breach discovery times: know your discovery tolerance

## 1. HIPAA Audits will continue

The 2012 HIPAA audits concluded, and the Department of Health and Human Services Office of Civil Rights, HHS OCR, will receive the evaluation results and recommendations in September 2013. OCR has stated that audits will continue in late 2013 or early 2014, HIPAA audits will become self-funded through Civil Money Penalties received, and that initial evaluation of these audits show that most covered entities did not maintain a continuous HIPAA program.

This will impact both covered entities and business associates in the short term, and businesses need to adapt to the new HIPAA landscape. For IT network and security, understanding what you have in place today can help you prepare for an audit and perform reasonable and appropriate protection of your PHI.

**Action:** Update relevant departments about the new HIPAA timelines and changes, so you can start to prepare.

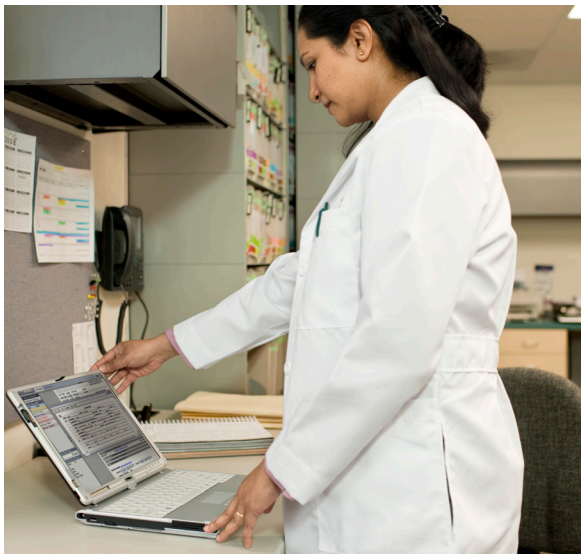
## 2. The HIPAA Audit Protocol and NIST 800-66 are your best preparation

HHS OCR has publicly posted the HIPAA Audit Program Protocol used during the 2012 HIPAA audits, so you can be prepared. There are three sections to this Audit Program Protocol – Privacy, Security, and Breach. For IT Security, the primary area to review and learn is the Security Protocol, which has 78 Key Activities, the Performance Criteria for each activity, and Audit procedure for each Key Activity. Because HIPAA is based on a self-assessment model, the Audit Program Protocol can give good guidance on how to self-assess, knowing that if an audit does occur at your organization, you are prepared on what to expect and how to respond.

**Action:** Identify someone on the network security team to become the technical lead on the HIPAA Audit Protocol and NIST 800-66 as it pertains to protection of electronic PHI.

## 3. Knowledge is a powerful weapon – know where your PHI is

Although not part of the HIPAA Security Rule, in the NIST 800-66 Revision 1 publication (Introductory Resource Guide for Implementing the HIPAA Security Rule), the first activity under the Administrative Safeguard is to 'identify all information systems that house Protected Health Information (PHI)'. Protecting critical data of any kind requires that you know where it is first so that you can protect it. For HIPAA, the critical data is PHI. For PCI, the critical data is credit card information. For many companies, critical data includes financial and accounting information. You can't begin to successfully protect PHI until you know where it is. Data discovery commonly yields some surprising findings about where data resides throughout the network environment. Servers, yes – but where are all those servers? Patient profile information, sure – but where is that information at any given time? Most likely, it is in more places than the servers. Registration and admissions departments, how many locations exist that can register and admit patients? Patient care – how many floors and computers and mobile devices use patient care information? Financial and Billing? Maybe. And where is that work done – in the office, by remote employees using their own computers? Studies, pilots, research? Where is that information created, stored, used? Know where your PHI is, and then you can properly protect it. Knowledge is a powerful weapon.



**Action:** Hire a consultant (or do it in house) to perform PHI data discovery throughout your network.

## 4. Risk Assessment drives your baseline

One identified result from the 2012 HIPAA Audits to date has been that most audited covered entities (95%) did not perform a Risk Analysis, also known as Risk Assessment, which is a Required Implementation Specification within the HIPAA Security Rule. The HIPAA Security Rule and Audit Protocol Program defines the Risk Assessment as "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."

A network risk assessment will identify which security gaps and vulnerabilities exist in the security implementation in the network. The gaps and vulnerabilities will impact the risk of PHI theft or loss. This information should play into the broader program risk assessment, so that you have the information you need to understand your current state of compliance and protection, and also to prioritize and develop a strategy to protect PHI and lead to HIPAA compliance. After knowing where your PHI is, the risk assessment, including the network risk assessment, is the critical next step towards PHI security.

**Action:** Build a risk assessment program that includes a network risk assessment, process and procedures assessment, and policy assessment.

## 5. Risk Management is continuous

You can look at the Risk Management implementation specification as the actions taken in response to the Risk Assessment. The HIPAA Security Rule defines Risk management (Required): “Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [§ 164.306(a)].”

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity 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.

One common mistake companies make in compliance in the network is that if they put the security programs, processes, and technologies in place, they think that compliance can be left behind. This makes compliance, and worse, effectively securing PHI (which is your critical data), a onetime effort that is then ignored. Risk management – reducing risk – needs to be a continuous activity. Implementing automation into network risk management becomes vital. Logs, alerts, attack prevention, and anomalous detection need to occur in real time and be intelligently coordinated.

**Action:** Understand how your risk reduction occurs, and what detection tools you have in place, and determine if those tools are effective.

## 6. Rely on security best practices

The general rule for the HIPAA Security Rule is to ensure the confidentiality, integrity, and availability of ePHI that is created, received, maintained, or transmitted [164.306(a)]. Protect against threats to PHI. That relates directly to network security best practices. So even though the HIPAA Security Rule doesn’t explicitly state the technology that should be used to meet the implementation specifications, security best practices rely upon a few well known and understood foundations: strong passwords, user authentication, firewalls, VPN encryption, and detection technologies. Those security best practices your network and security teams have in place most likely are already being used to protect some of your PHI. Those same practices can be used to help you address HIPAA compliance as well. Rely on what you have and supplement what you need. But rely on the security best practices, not on compliance requirements, to drive protection of your PHI and other critical data.

**Action:** Learn the security best practices your teams have in place that can be used for protection of PHI and HIPAA compliance.

## 7. Ignorance is not bliss

Gone are the days of using the excuse “I didn’t know, so I’m not accountable” for data breaches and PHI theft. The penalty tiers of the HIPAA Omnibus Final Rule clearly articulate that you will pay for ignorance moving forward. The penalty scheme comprises four tiers, shown in Table 1, adopted from the HITECH Act:

- **Tier 1** – a violation that the covered entity did not know about, and while exercising reasonable diligence, would not have known that the covered entity violated a provision
- **Tier 2** – a violation that was due to reasonable cause and not to willful neglect
- **Tier 3** – a violation was due to willful neglect and was timely corrected
- **Tier 4** – a violation was due to willful neglect and was not timely corrected

**Table 1.** Categories of Violations and Respective Penalty Amounts Available

| Violation Category | Each Violation | All such violations of an identical provision in a calendar year |
|---|---|---|
| (a) Did Not Know | $100 – $50,000 | $1,500,000 |
| (b) Reasonable Cause | $1,000 – $50,000 | $1,500,000 |
| (c) (i) Willful Neglect-Corrected | $10,000 – $50,000 | $1,500,000 |
| (c) (ii) Willful Neglect-Not Corrected | $50,000 | $1,500,000 |

Many organizations interpret this to mean that their maximum penalty per year is $1.5 Million. However, the industry has seen several situations in 2012 and 2013 that the amount paid is much greater than this. This penalty structure is for each violation, with a maximum for that specific violation. For example, if someone loses a laptop and it has unencrypted PHI, the result could be a $1.5 million penalty. If data is then stolen from a server in the data center that is a different violation and would also be subject to penalties that have a maximum of $1.5 million.

Plausible deniability does not mean that your organization would definitely fit into the “Did Not Know” category. That category also states that it requires reasonable due diligence and still would not have known. If you refer back to the previous Know where your PHI is, Risk Assessment and Risk Management considerations, and you don’t know where PHI is in your network, or you don’t understand what your network vulnerability and gaps are, or you are not protecting your PHI against anticipated threats; you may find yourself in one of the Willful Neglect categories. And then ignorance is bliss can become very costly.

Network security best practices not only help to keep PHI safe, but they also may reduce the costs of penalties if a breach does occur. Your network is a critical place to exercise reasonable due diligence, and it is also your weapon to defend against beaches and electronic PHI theft from your network environment.

**Action:** Understand the potential costs to your organization due to a breach of PHI, and learn how to use what you have in your network today to reduce those costs and risk.

## 8. Your business associate(s) must be tracked

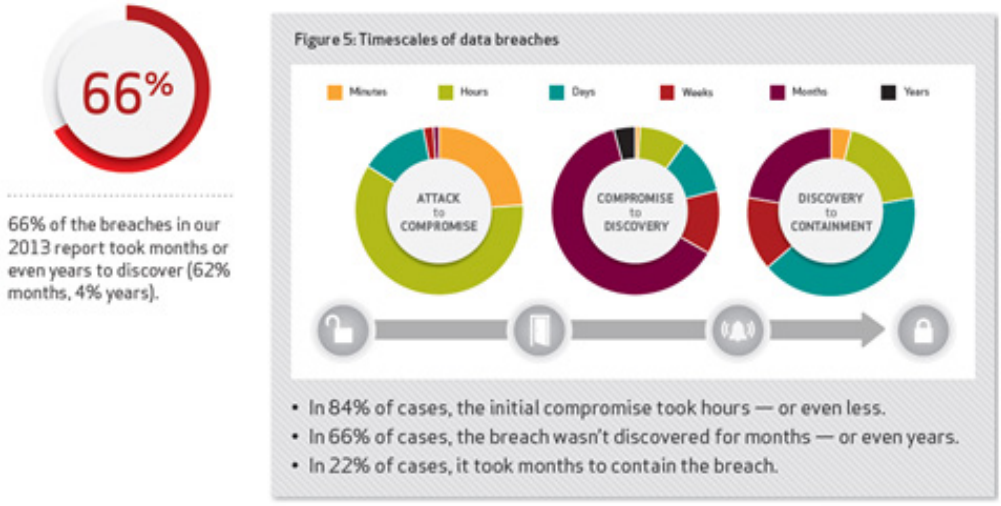
The HIPAA Omnibus Final Rule changed the Business Associate definition, and now makes Business Associates obligated to comply with HIPAA. You most likely will have more business associates than previously, and those business associates that do have access to your network and/or your PHI data need to perform the same steps towards achieving HIPAA compliance and protecting your PHI as you do. The Ponemon Institute’s Third Annual Benchmark Study on Patient Privacy and Data Security (December 2012), reveals that 42% of the breaches involved a third party “snafu.” And although the business associate would ultimately be responsible for a breach or theft of PHI caused by them, it is your patients and clients that will suffer, and your reputation that will suffer. While your business associates are on your network, how do you know what they are doing? Do you have tracking, logging, and access controls in place so that they can only access the information their job function requires and not other data?

**Action:** Identify which partners and vendors will now be considered Business Associates in the new HIPAA landscape. Include those relationships as part of your Risk Assessment, and include any network connections to those entities as part of your network risk assessment.

## 9. Breach discovery times: know your discovery tolerance

From the 2013 Verizon Data Breach Investigations Report (see Figure 1 below), two thirds of the compromises were not discovered for months, or longer. What is your tolerance for “not knowing?” Can that discovery time tolerance be justified through reasonable due diligence, or are you back at the "ignorance is bliss” phase, which could be interpreted as Willful Neglect in the case of a breach of PHI?

**Figure 1.** Not Knowing is Painful




Source: Verizon 2013 Data Breach Investigations Report

Detection of strange behavior, network anomalies, and network traffic spikes targeted at specific device(s) can all help to reduce the time between compromise and discovery of a breach of PHI in the network. Reducing your discovery time can reduce your costs around breach notification, penalties, and remediation costs caused by a breach.

**Action:** Determine your discovery time tolerance and identify steps to reduce your compromise-to-discovery times.

Cisco’s Compliance team focuses on helping customers simplify meeting mandated HIPAA, Sarbanes-Oxley Act of 2002 (SOX) and Payment Card Industry (PCI) compliance requirements. Our approach provides a foundation for layering in new technologies, helping to enable customers to keep pace with the rapid change in areas like mobile technology and cloud computing that are important to health care providers and others while maintaining the underpinning of a secure architecture. To learn more about Cisco® compliance solutions, please visit http://www.cisco.com/go/compliance.


Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.





Printed in USA DR/LW-18774 05/13