

# HIPAA and Beyond

How to Effectively Safeguard Electronic Protected Health Information

Ben Rothke, CISSP PCI QSA

August 4th, 2008



## Introduction

In the world of information security, well-defined security programs are the forests, and regulations like HIPAA, SoX and PCI are the trees. And too many healthcare organizations mistake the forest for the trees.

By way of analogy, one of the benefits of Social Security is SSI or *Supplemental Security Income*. The operative word is *supplemental*. Social Security is meant to augment your retirement, not be the main income source for your retirement. HIPAA is much like SSI and meant to supplement your formal information security program. If you view HIPAA as the end-all of your information security and privacy program, you are in huge trouble.

This white paper will detail how to go beyond HIPAA by showing how to use HIPAA as the starting point for your security program, and then using best practices and Lumension Security solutions to improve your overall security posture.

## HIPAA – Showing its Age

Imagine paying \$1.25 for a gallon of gasoline. One would have to go all the way back to 1996 to get that price. Going back to 1996 also takes us to the year when Congress enacted the Health Insurance Portability and Accountability Act (HIPAA).

HIPAA was created for health insurance reform and the streamlining of claims, and not about security and privacy. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA known as the Administrative Simplification provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

Administration Simplification provisions also address the security and privacy of patient health data. The HIPAA security and privacy rules are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the US health care system.

## HIPAA Security and Privacy Rule

Within Administration Simplification exists the

*HIPAA Privacy Rule and Security Rule*. The Privacy Rule became effective in April 2003 and establishes regulations for the use and disclosure of Protected Health Information (PHI). PHI is broadly defined as any information about the health status, provision of health care, or payment for health care that can be linked to an individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history<sup>1</sup>.

The HIPAA security rule was issued in February 2003 and complements the Privacy Rule. While the Privacy Rule pertains to all PHI, including paper- and electronic-based, the Security Rule deals specifically with electronic PHI (E PHI) and lays out three types of security safeguards required for compliance: *administrative*, *physical* and *technical*. For each, the Rule identifies various security standards, and for each standard, it names both required and addressable implementation specifications.

## Moving Beyond HIPAA

HIPAA was created by non-security personnel, who likely could not differentiate between a fire-wall and fire extinguisher. The outcome is that HIPAA lacks the depth and breadth on which to build an information security program. If you build your security and privacy program with HIPAA solely as its foundation, it will fail as HIPAA takes a myopic view of security and privacy with PHI being the center of its universe. But there is much more to information security than PHI.

With that, covered entities<sup>2</sup> (CE) must look beyond HIPAA and focus globally if they want more than simply HIPAA compliance.

While the intent of HIPAA was valorous, over a decade has passed since its initial inception and it has already begun to show its age. Organizations that mistakenly look to HIPAA for their security infrastructure should stop being shortsighted and look forward.

While HIPAA is a static regulation, CE's exist in a dynamic IT world with new threats coming about daily. When HIPAA first came out, vulnerability assessments, patching and configuration remediation were only typically performed quarterly at best. Now with zero-day threats, lack of a defined network perimeter and focus on information

protection, the need for real-time patching and proactive endpoint and data protection is a basic requirement.

The following steps in this white paper will show you how to get that global view and how to move beyond HIPAA for any CE.

### **Step 1 - Using a Framework for Security**

The healthcare industry doesn't have a lack of information security products at its disposal. Data centers are stocked full of racks of firewalls, VPN's, security appliances and much more. While the underlying infrastructure is there, the challenges CE's face is making these products work together, to provide adequate security, and to support their HIPAA compliance effort.

By employing a well-developed, organized and enforced set of security policies, and by understanding where your exposures reside, you will be better prepared for issues when they occur. Organizations that do not define and enforce security policies proactively are in for a rough time when disaster strikes. Simply put, if your security infrastructure isn't built on a solid foundation, it is bound to collapse under the weight of increased threats and vulnerabilities. By creating a security foundation, CE's can easily deal with any new regulation.

This is especially true given the compliance 80/20 rule. If you take all of the security and privacy regulations and combine them, there is roughly an 80% commonality between them. The 80/20 rule shows that having a core framework in place to deal with the 80% commonality means that at worst an enterprise will only have 20% of the new regulation to deal with.

That is where information security frameworks come into the picture. An information security framework contains the assumptions, concepts, risk values, and security practices underlying an organization's information security infrastructure. Frameworks such as ISO 27001<sup>3</sup> and 27002<sup>4</sup> and ITIL<sup>5</sup> (IT Infrastructure Library) are needed because current healthcare security projects are much more complex than those of years past. Frameworks provide the formal approach to security, especially since too many CE's take an ad hoc approach to security, which is an abomination to every security professional.

Using frameworks such as ISO-17799 or ITIL helps CE's by giving them a structure with which to protect their IT assets. Also, when an organization decides to formally embrace a framework, it sends a strong message of its commitment to information security.

Within HIPAA, using a framework can be especially valuable as it can show others the depth of your security program, and your overall commitment to their security and privacy. As security is becoming a differentiating factor, the use of a framework can differentiate your organization from insecure ones.

### **Step 2 – Risk Assessment**

The foundation of any information security program must be a formal and comprehensive risk assessment. If you don't know your risks, you have no idea of your security context, no idea of who your adversaries are, and in essence, you are shooting in the security dark. CE's that jump into doing information security without a comprehensive and formal risk assessment end up doing a lot of security stuff, but don't have much to show for it when all is said and done. To properly protect your network, you need to create a matrix detailing the risks your organization faces, listing the level of the threat against the likelihood of it happening.

Once the risk assessment is complete, don't make the mistake of attempting to quickly fix all of the problems by creating a huge to-do list and then giving it to external consultants to complete. The only way to effectively manage risk on enterprise networks is to approach the remediation process in a formal strategic manner - create detailed project plans under the control of an effective project manager.

The beauty of a risk assessment is that it tells you exactly what you need to worry about. If you don't take this approach, you end up defending against murky hackers and vague threats from somewhere. A formalized risk assessment gives you the knowledge to know who your enemy really is; Sun Tzu would be proud.

A risk assessment is the ultimate commitment to HIPAA, as it shows that a CE isn't simply trying to take a rubber stamp approach to HIPAA, rather they are trying to get to the core of the security and privacy issues. More importantly, it shows

that a CE is focusing on the real threats, rather than on perceived external threats.

### Step 3 – The 3 P's (Policy, Processes, Procedures)

CE's need information security policies to ensure a safe and sound infrastructure. Security policies are often the first step in ensuring that corporate assets are not squandered by some nefarious employees. Security policies are like fiber, that is, the kind you eat. Everyone agrees that fiber is good for you, but no one really wants to eat it - so too with information security policies. They are sorely needed, but most users don't go out of their way to comply with them. And in many CE's, they are not even trained in what they have to do. But failure to have adequate information security policies can lead to myriad risks for a CE.

The centrality of information security policies to virtually everything that happens in the information security field is increasingly evident. For example, system administrators cannot securely and effectively install a firewall unless they have received a set of clear information security policies. These policies will stipulate the type of transmission services that should be permitted, how to authenticate the identities of users, and how to log security-relevant events.

Similarly, an effective information security training and awareness effort cannot be initiated without first writing information security policies, because policies provide the essential content upon which training and awareness material rely. It is for these reasons that every major regulation or standard relating to information security and/or data privacy specifically requires written security policy documents.

A comprehensive set of security policies are required to map abstract security concepts to the real world implementation of your security solutions as policy defines the aims and goals of the CE.

Security processes can help a CE optimize their IT security infrastructure. The more complex an organization's IT security infrastructure becomes, the more important it is to follow consistent and formal security operational processes and policies.

Effective procedures ensure a standard level of

configuration consistency within your organization. The benefits of Standard Operating Procedures (SOP) are immense and include:

- Standardize operations among divisions and departments
- Reduce confusion
- Designate responsibility
- Improve accountability of personnel
- Record the performance of all tasks and their results
- Reduce costs
- Reduce liability

There are many sources for SOP's, some of which include:

- [ISO 17799](#)
- [CoBIT](#)
- [NIST 800 series](#)
- [Standards for Security Categorization of Federal Information and Information Systems \(FIPS 199\)](#)
- [ITIL](#)

### Step 4 – Training and Awareness

Effective information security training and awareness effort can't be initiated without first writing information security policies which provide the essential content for training and awareness materials. Establishing clear expectations through an information security awareness program is a critical element of an effective and enforceable set of policies.

Awareness is specifically required in HIPAA section § 164.308 Administrative safeguards, which states in section (5)(i) *Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).*

So important is awareness that [The Standard of Good Practice for Information Security](#) from the [Information Security Forum](#) (ISF) writes that specific activities should be undertaken, such as a security awareness program, to promote security awareness to all individuals who have access to the information and systems of the organization, with the objective to ensure all relevant individuals apply security controls and prevent important information used throughout the organization from being compromised or disclosed to unauthorized individuals.

The ISF defines security awareness as the ex-

tent to which staff understand the importance of information security, the level of security required by the organization and their individual security responsibilities.

One of the major problems with all information security policies revolves around management not knowing whether users have read and understood the policies. If users have not read the policies, they may ignorantly do things that cause security problems, for example, opening a file sent as an email attachment without scanning the file with a virus detection package. If users have read the policies, but not sufficiently understood them, they may do things that cause security problems.

The true test of understanding would be observation in real-world working environments, but that is too expensive for many CE's. As the next best thing, users can be tested to determine that they understood the policy, and if they pass a quiz, then access privileges may be granted. For example, a worker who wanted to telecommute could read the telecommuting security policy, take a quiz, and get a passing score, at which point management would authorize the user to gain access to the organization's internal network over the Internet using a virtual private network. In sophisticated organizations, such privileges may be enabled automatically based on a quiz delivered through an intranet computer-based training system or software.

## Moving Beyond HIPAA

Once you take care of the above fundamental steps, go full-steam into HIPAA compliance. It is also important to do these steps before using a solution. But once that is done, Lumension's suite of proactive security solutions can help in your HIPAA program to ensure that confidential medical records, specifically patient health information, remain secure.

Endpoints, especially ones that move on and off the network, are extremely vulnerable to data threats as their configurations drift over time and not kept up-to-date with the latest anti-virus and operating system and application patches. Add to this unmanaged removable media (podslurpers) and insecure applications, which together can easily open the floodgates for data to escape into the wrong hands, whether intentionally or accidentally.

The fact that so many endpoints are infested with spyware, keyloggers and other types of malware, which so easily compromise the integrity and confidentiality of patient information, should give any CIO pause.

Lumension Security's Proactive Security Suite ensures ePHI privacy by providing the necessary controls to manage the data flowing to and from network endpoints and by rapidly securing endpoint configurations and patching and remediating software vulnerabilities that could leave IT assets and sensitive data exposed. Some of these solutions include:

Solution	Benefits
Lumension Security Vulnerability Management	<ul style="list-style-type: none"> <li>• Complete network-based scanning solution enables assessment and analysis of threats impacting all network devices.</li> <li>• Proactive management of threats through automated collection, analysis, and delivery of patches (all major operating systems and applications) across heterogeneous networks.</li> <li>• Out-of-the-box regulatory and standards-based assessment to ensure endpoints are properly configured.</li> <li>• Custom remediation capabilities to address configuration issues, remove unauthorized files and applications, address zero-day threats, patch custom software and more.</li> </ul>
Lumension Security Endpoint Protection	Policy-based enforcement of application use to secure your endpoints from malware, spyware and unwanted or unlicensed software.
Lumension Security Data Protection	Policy-based enforcement of removable device use to control the flow of inbound and outbound data from your endpoints.
Lumension Security Reporting and Compliance	Robust data warehouse that enables easy creation and sharing of reports on all aspects of your security efforts in support of policy compliance.

The following table lists just some of the many benefits in which Lumension Security's Proactive Security Suite helps CE's:

Main Benefit	Other Benefits
Comply with HIPAA requirements for safeguarding the integrity and availability of ePHI	<ul style="list-style-type: none"> <li>• Reduce the risk of ePHI from being improperly disclosed</li> <li>• Prove compliance with HIPAA by providing a detailed audit trail of all device and application execution attempts, by tracking data that is copied to and from removable devices and by controlling what data is allowed to be copied to a device at the file level</li> <li>• Patch and remediate vulnerabilities before they can be exploited to access ePHI</li> <li>• Control and monitor the flow of inbound and outbound ePHI with removable media and devices</li> <li>• Identify organizational security holes in the protection of ePHI through comprehensive auditing capabilities</li> </ul>
Prevent malware execution originating at an endpoint	<ul style="list-style-type: none"> <li>• Protect against network security breaches where ePHI could be exposed to fraud</li> <li>• Enable the transmission, integrity, confidentiality and retention of ePHI without disruption, corruption or loss</li> </ul>
Improve IT system performance	<ul style="list-style-type: none"> <li>• Prevent unwanted applications and devices from burdening network bandwidth</li> <li>• Enable faster computing resources on network, laptops and PCs</li> <li>• Maintain PCs' performance as new with configurations remaining stable</li> </ul>
Reduce endpoint security TCO	<ul style="list-style-type: none"> <li>• Minimize security or HIPAA compliance crisis response</li> <li>• Remediate vulnerabilities more quickly and with fewer required resources</li> </ul>
Improve end user productivity	<ul style="list-style-type: none"> <li>• Block unwanted, non-business applications</li> <li>• Enforce policy to ensure endpoints run as expected</li> </ul>

## Conclusion

Security and the protection of PHI is more than just firewalls and encryption. By having this broad approach, and rising above the minimal protection that HIPAA offers, CE's can ensure that they are HIPAA compliant not only with the letter of the law, but more importantly, the spirit of the law.

### About the Author

Ben Rothke CISSP, PCI QSA ([ben@rothke.com](mailto:ben@rothke.com)) is a New York based Security Consultant and the author of [Computer Security: 20 Things Every Employee Should Know](#) (McGraw-Hill, 2006).

### About Lumension Security™

Lumension Security™, formed by the combination of PatchLink® Corporation and SecureWave® S.A., is a recognized, global security management company, providing unified protection and control of enterprise endpoints for more than 5,100 customers and 14 million nodes worldwide. Leveraging its proven Proactive Security Model, Lumension Security enables organizations to effectively manage risk at the endpoint by delivering best-of-breed, policy-based solutions that simplify the entire security management lifecycle. This includes Vulnerability Management, Endpoint Protection, Data Protection and Reporting & Compliance. Headquartered in Scottsdale, Arizona, Lumension has offices worldwide, including Virginia, Florida, Luxembourg, the United Kingdom, Spain, Australia, Hong Kong and Singapore.

### Lumension Security™, Inc.

**15580 N. Greenway-Hayden Loop, Suite 100  
Scottsdale, AZ 85260**

[www.lumension.com](http://www.lumension.com)

#### Footnotes:

1. This is due in part since it is relatively easy to correlate unrelated data.
2. Any organization that routinely handles protected health information in any capacity is in all probability a covered entity.
3. ISO/IEC 27001 is the formal standard against which organizations may seek independent certification of their Information Security Management Systems (meaning their frameworks to design, implement, manage, maintain and enforce information security processes and controls systematically and consistently throughout the organizations).
4. ISO/IEC 27002 provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining Information Security Management Systems (ISMS).
5. ITIL is a customizable framework of best practices designed to promote quality computing services in the information technology sector.