

HEALTHCARE AND COMPLIANCE— THE NEW REALITY

Regulatory Compliance Enabled by Juniper Networks
Security Solutions

Table of Contents

Executive Summary	3
HIPAA	4
HIPAA Compliance Requirements	4
Table 1. HIPAA Security Standard Safeguard Categories	4
HIPAA Enforcement	5
How Your Network Can Promote HIPAA Compliance	6
Granular Access Control	6
Secure Remote Access	7
High Security	7
The HITECH Act	7
The Carrot and the Stick	7
The Cost of an Unsecured Breach	8
How Your Network Can Help Prepare You for HITECH	8
Measurable Security	8
Increased Volume	9
PCI DSS	9
The Really Big Stick	9
What is PCI DSS?	9
How is PCI DSS Different?	10
Table 2. HIPAA and PCI DSS Comparison	10
Table 3. PCI DSS Goals and Requirements	10
What about PCI DSS Enforcement?	11
How Your Network Can Help Prepare You for PCI DSS	11
Logging and Reporting	11
Granular Secure Access Regardless of Location	11
Firewalls and Intrusion Prevention	12
Conclusion	12
About Juniper Networks	13

List of Tables

Table 1. HIPAA Security Standard Safeguard Categories	4
Table 2. HIPAA and PCI DSS Comparison	10
Table 3. PCI DSS Goals and Requirements	10

Executive Summary

Anyone can see that healthcare has changed dramatically over the last 20 years. Gone are the days when patients would see one physician for much of their life and would seldom see specialists outside that doctor's care/supervision. In yesterday's healthcare facilities, the support staff was stable, ancillary work such as billing was performed in-house, and virtually all services were handled in one place, by people. In today's environment, patients may see a different doctor at every visit. Specialists abound, and they are often at different locations. Support staff is highly mobile and may be transient, while many ancillary services are provided by third parties outside the hospital or clinic. Today's healthcare environment features services that are more distributed (both physically and computationally) and designed to serve more audiences, using a host of disparate devices that may not be optimized to work together. A growing number of critical applications reside in the cloud and aren't even housed on the network.

Today's patient has changed as well. Where once trust was put into an individual, more credence is now given to the facility where care is delivered, as well as to the technology that is housed there. Hospitals, once a single building entity, have become "healthcare systems." This has created a growing sense of brand consciousness which, while not new to healthcare, has previously been more focused on individuals within the system. Patients as a whole are also becoming more technologically savvy as services move to the Internet, and more transactions/communications move online.

As much as healthcare has changed on the outside, however, possibly the biggest paradigm shift in the industry has taken place behind the scenes. Increasingly critical IT networking functions, designed to be the tool for delivering better care, can collide with the needs of healthcare as a cost sensitive and highly competitive business. From an IT point of view, few environments are more challenging than healthcare, with issues that include a demanding and unusual set of applications and devices, such as:

- Patient telemetry and bedside monitoring
- Electronic medical records (EMRs)
- Picture archiving and communication systems (PACS)
- Medical equipment monitoring
- Location and asset tracking
- Barcode medication administration
- Converged voice and data
- Supplemental "for fee" services available in room or in guest areas

As more sensitive information moves onto the network and into the cloud, the complete security, privacy, and regulatory compliance of such information must be assured. Given the history of security breaches in areas like finance and retail, it was only logical that there would be regulatory bodies passing specific legislation to safeguard patients and their information. In fact, the first federal regulation, Health Insurance Portability and Accountability Act (HIPAA), actually preceded some of the best known public data breaches in other sectors. In this paper, we will look at three mandates of note in healthcare today:

1. HIPAA, a by now familiar set of security and privacy restrictions specific to the healthcare field
2. The HITECH Act, which features federal funding to enable electronic health records, as well as significant penalties, if this action is not done securely
3. Payment Card Industry Data Security Standard (PCI DSS), a comprehensive set of regulations designed to ensure the privacy of credit card holder's financial data

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was passed into law in August 1996, placing new requirements on thousands of U.S. organizations involved with the provision of healthcare. Its two principle aims are: (1) to increase availability of healthcare by standardizing the exchange of information, and (2) to protect the confidentiality and security of patient records. Organizations that must comply with HIPAA are known as covered entities. These include health plans (e.g., HMS, group health plans), healthcare clearinghouses (e.g., billing and repricing companies), and healthcare providers (e.g., doctors, dentists, hospitals). The HIPAA Privacy Rule came into effect in April 2001, requiring covered entities to come into compliance by April 2003. This rule formalized procedural restrictions on the handling of healthcare information.

HIPAA's effect on IT requires that an organization must secure all digital data related to an individual's healthcare, referred to as electric protected health information (ePHI), regardless of the location of the data. This means that to be HIPAA compliant, organizations must take steps to prevent inappropriate access to ePHI by putting into place both proactive and reactive control over IT systems.

HIPAA Compliance Requirements

HIPAA security standards combine network security and implementation specifications. There are two types of implementation specifications: *Required and Addressable*. If "Required," organizations must implement the specification. If "Addressable," organizations must assess whether or not the specification is a reasonable and appropriate safeguard in their environments when analyzed with reference to the likely contribution for ePHI protection. An amended version of the security standard is presented below. The security standards are categorized into three broad safeguard categories: *Administrative Safeguards, Physical Safeguards, and Technical Safeguards*.

Table 1. HIPAA Security Standard Safeguard Categories

STANDARDS	SECTIONS	IMPLEMENTATION SPECIFICATIONS (R) = REQUIRED (A) = ADDRESSABLE
Administrative Safeguards		
Security management process	164.308(a)(1)	Risk analysis (R) Risk management (R) Sanction policy (R) Information system activity review (R)
Assigned security responsibility	164.308(a)(2)	(R)
Workforce security	164.308(a)(3)	Authorization and/or supervision (A) Workforce clearance procedure (A) Termination procedures (A)
Information access management	164.308(a)(4)	Isolating healthcare (A) Clearinghouse function (R) Access authorization (A) Access establishment and modification (A)
Security awareness and training	164.308(a)(6)	Response and reporting (R) Protection from malicious software (A) Login monitoring (A) Password management (A)
Security incident procedures	164.308(a)(6)	Response and reporting (R)
Contingency plan	164.308(a)(7)	Data backup plan (R) Disaster recovery plan (R) Emergency mode operation plan (R) Testing and revision procedure (A)
Evaluation	164.308(a)(1)	(R)
Business associate contracts and other arrangement.	164.308(b)(1)	Written contract or other arrangement (R)

STANDARDS	SECTIONS	IMPLEMENTATION SPECIFICATIONS (R) = REQUIRED (A) = ADDRESSABLE
Physical Safeguards		
Facility access controls	164.310(a)(1)	Contingency operations (A) Facility security plan (A) Access control and validation procedures (A) Maintenance records (A)
Workstation use	164.310(b)	(R)
Workstation security	164.310(c)	(R)
Device and media controls	164.310(d)(1)	Disposal (R) Media reuse (R) Accountability (A) Data backup and storage (A)
		Media reuse (R)
		Accountability (A)
		Data backup and storage (A)
Technical Safeguards (see § 164.312)		
Access control	164.312(a)(1)	Unique user identification (R) Emergency access procedure (R) Automatic logoff (A) Encryption and decryption (A)
Audit controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to authenticate (R) Electronic protected health information (A)
Person or entity authentication	164.312(d)	(R)
Transmission security	164.312(e)(1)	Integrity controls (A) Encryption (A)

Source: 45 CFR Parts 160, 162, and 164 -Health Insurance Reform: Security Standards; Final Rule, 2/20/2003

HIPAA has been widely criticized for not having sufficient “bite.” According to Forrester, “...the healthcare industry... largely ignored many of the requirements laid out in HIPAA. Why? Because first, there were neither real incentives to comply with these requirements nor penalties for noncompliance, and second, nobody was enforcing HIPAA.” In many cases, infractions that have resulted in fines have occurred only because the breaches were publicly identified and therefore had to be addressed. Part of the issue is that while every organization wants to be secure, HIPAA provides only very general guidelines on how to achieve that goal. All healthcare organizations that are classified as “covered entities” by HIPAA must demonstrate “reasonable” efforts to comply with HIPAA’s privacy and security aspects, but such a broad requirement can leave much room for interpretation. HIPAA defines goals, but leaves it up to the organization to determine how to reach them. This is deliberate; according to Gartner, “The rule was developed to be flexible to exploit maturing industry best practices, scalable so that it could be used effectively with organizations of all sizes, and technology-neutral so that future technologies could be used without changing the standard.” While these are admirable goals, complying with a nonspecific standard can sometimes be more difficult than a simple check box.

Still another issue with HIPAA compliance is the fact that healthcare records can be accessed from any number of places, all the way from hospital staff tapping into databases to malicious outsiders hacking their way into a system and mining for valuable personal information. Many different users require access to do their jobs, but the more open the network becomes, the more arduous it is to secure. Because provider partners must constantly share patient information, it can be difficult to untangle where an infraction actually occurred, much less prevent one.

HIPAA Enforcement

U. S. Department of Health and Human Services (HHS)’s Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy and Security Rules. Enforcement of the Privacy Rule began April 14, 2003 for most HIPAA covered entities. HIPAA covered entities were required to comply with the Security Rule beginning on April 20, 2005. OCR became responsible for enforcing the Security Rule on July 27, 2009.

As of May 2010, the Department of Health and Human Services reports that “since the compliance date in April 2003, HHS has received over 52,414 HIPAA Privacy complaints. We have resolved over ninety percent of complaints received (over 46,958): through investigation and enforcement (over 10,956); through investigation and finding no violation (5,694); and through closure of cases that were not eligible for enforcement (30,308).

From the compliance date to the present, the compliance issues most frequently investigated include:

1. Impermissible uses and disclosures of protected health information
2. Lack of safeguards of protected health information
3. Lack of patient access to their protected health information
4. Uses or disclosures of more than the minimum necessary protected health information
5. Complaints to the covered entity

Since OCR began reporting its Security Rule enforcement results in October 2009, HHS has received approximately 105 complaints alleging a violation of the Security Rule. During this period, the organization closed 40 complaints after investigation and appropriate corrective action. As of May 31, 2010, OCR had 157 open complaints and compliance reviews.

As an example of what HIPAA violations can actually represent, the Federal Trade Commission approved the final consent order in June, 2009, settling charges that CVS Caremark violated HIPAA in 2006, when pharmacy workers discarded pill bottles, medication instruction sheets, and computerized order information into open trash containers. As part of the final order, the company, which operates about 6,300 retail pharmacy stores, must designate an employee to create a comprehensive written “get-well” plan, submit to assessments every other year for 20 years, and was ordered to pay \$2.25 million in fines. On a smaller scale, Community Hospital of San Bernardino has been fined \$325,000 for breaches of more than 200 patient records by employees, while the UCLA Medical Center has moved to fire 13 employees and suspended six others for unauthorized access to confidential medical records of pop star Britney Spears in 2008. And the regulation will only continue to become better enforced, as the HITECH Act takes hold. This is because benefits promised by HITECH are only available to facilities that meet standards. It is also worthwhile to note that, according to Gartner, “Organizations found in violation of HIPAA-mandated security measures will incur penalties and collateral damages 10 to 20 times higher than the cost of HIPAA security compliance.”

How Your Network Can Promote HIPAA Compliance

Granular Access Control

While the HIPAA statutes are not limited to the network, as seen in the CVS case, the network does have an important part to play. The first issue to consider is the central conflict between an open network that provides access to users with a legitimate need, and a closed network where security is locked down. This issue is perhaps greater in healthcare than in many industries, since there are such a variety of workers, settings, and types of information. Because technology is such an integral part of healthcare, there is a legitimate need to control access in a very granular fashion.

A strong network access control (NAC) system can go a long way toward providing the security needed, while ensuring that those with a legitimate need for assets can get to them. Unfortunately, many NAC solutions require a disruptive and costly set of network/equipment upgrades, particularly if the solution is proprietary. Providers should consider an access control system that uses elements that are in the network already, such as firewalls or intrusion prevention systems (IPS), and includes such standard protocols as 802.1X. It is also a good idea to look for a solution that is designed to enable a phased rollout, so additions can be made and changed in a gradual, systematic manner that enables changes to be propagated throughout the network as you go. Finally, an optimal NAC solution for healthcare providers should be capable of extending information beyond the confines of the LAN, enabling a combination of strong authentication and ease of use.

Find out more about the ways that Juniper Networks® Unified Access Control can help by clicking here: www.juniper.net/us/en/products-services/security/uac/.

Secure Remote Access

Workers must have access to network servers, PHI databases, and stored information regardless of their location. This access must feature both strong authentication and authorization, so that users can only reach the information that they require. Because many of these users are not IT specialists, the system must be easy to provision and use. Also, many medical professionals use smartphones that house sensitive patient information, and as these devices become more like mobile computers, they must be protected in the same way. Business associates, who also need access to PHI/ePHI, must be considered as well.

SSL VPNs provide an ideal solution to these requirements. The right SSL VPN should feature extremely granular access to authorized users. It should accommodate virtually any authentication method/scheme, from simple passwords for insecure assets to multi-factor or biometric systems. The SSL VPN should also work with a variety of standard authorization systems. Security should extend to smartphones, enabling secure remote access from a variety of devices. A premier solution would also enable user information sharing between the NAC system and the SSL VPN, allowing a user to move seamlessly from one location to another. Another factor to consider is the degree to which the SSL VPN can be used to set up extranets for allied health professionals in a simple, easy to use fashion.

Find out more about the ways that Juniper Networks SA Series SSL VPN Appliances can help by clicking here: www.juniper.net/us/en/products-services/security/sa-series/.

High Security

A trend not limited to healthcare is that attacks are becoming more sophisticated and more personally intrusive. As we have witnessed recently in the press, personal information theft has become high profile and costly. Businesses have lost their credibility with relaxed network security and risk the potential of being forced out of business bad publicity. Healthcare networks face the same predicament with the risk of having to make public disclosures of the compromise of highly sensitive and private information stored and transacted on a daily basis when a similar breach occurs. The confidentiality of PHI on the network, and the credibility of the healthcare institution as a whole, are placed at great risk without proper security implementations. This is an area of concern that can be addressed in part with network accountability and threat mitigation.

The fact is that due to the sophistication of today's attacks, there is no such thing as a single security product that will catch every threat. To best ensure security, look for a modular solution made up of products that are best-in-class by themselves, but can also work together. These solutions empower the security stance of the network itself to change based on parameters you set, as variables within the user environment, application type, and threat landscape evolve over time. Central policy creation and deployment through a single platform will greatly minimize both the time to deploy a system as well as the chance of human error. Finally, the ideal solution should also correlate events from throughout the extended network. Not only will this combination of features provide a closed loop on security and network activities, it is vital in proactively compiling required compliance reports.

Find out more about how Juniper Networks Adaptive Threat Management Solutions can help by clicking here: www.juniper.net/us/en/solutions/public-sector/security-compliance/adaptive-threat-management/.

The HITECH Act

The Carrot and the Stick

The Health Information Technology for Economic and Clinical Health Act (HITECH) is part of the American Recovery and Reinvestment Act of 2009 (ARRA). The HITECH Act is intended to encourage more effective and efficient healthcare through the use of technology, thereby reducing the total cost for all Americans and enabling greater access to the system. The HITECH Act appropriated \$250 million in 2009/2010 for the implementation of new provisions to expand the use of health information technology (HIT). The HITECH Act features significant financial incentives to providers for implementing HIT, in particular, electronic health records (eHR).

The United States is making this investment with the expectation that every citizen will have an electronic medical record by the year 2014. The Act also provides individuals with the right to obtain their PHI in electronic format. Any provider expecting to participate in the Act's incentives should be prepared to deliver on these requests or could risk a finding that their use does not qualify as "meaningful use."

Because this legislation anticipates a massive expansion in the exchange of electronic protected health information (ePHI), the HITECH Act also widens the scope of privacy and security protections available under HIPAA, increases the potential legal liability for noncompliance, and provides for more enforcement. Business associates are also required to comply with HIPAA's Security Rule, expanding the scope of the issue even further. The HITECH Act contains mandatory penalties for "willful neglect." Although enforcement will vary case by case, it is likely that providers without a compelling reason for noncompliance could be at risk. Moreover, civil penalties for willful neglect can extend up to \$250,000 under the HITECH Act, with repeat and/or uncorrected violations extending to \$1.5 million.

But fines may not be the biggest stick carried by HITECH. The law adds a provision requiring a formal investigation if a preliminary investigation suggests possible willful neglect; a tiered increase in the monetary amount of civil penalties that may be assessed in a year for various determinations; and enforcement by the state attorneys general. Perhaps more damaging, however, given the increasingly brand conscious, tech savvy nature of today's patients, is the fact that HITECH Act imposes data breach notification requirements for unauthorized uses and disclosures of "unsecured PHI." The Act defines unsecured personal health information as PHI that has not been secured by using a technology or methodology specified by HHS guidance—specifically those that render PHI as unusable, unreadable, or indecipherable to unauthorized individuals and is endorsed by an accredited standards organization like the National Institute of Standards and Technology (NIST).

The Cost of an Unsecured Breach

Disclosure requirements are similar to those imposed by states related to financial information, in that they require that patients be notified of any unsecured breach. If a breach impacts 500+ patients, then Health and Human Services must be notified; certain conditions may also trigger notification of local media. According to independent research by Ponemon Institute, while the average customer "turnover" or "churn" due to a data breach was generally 3.6%, in healthcare it was much higher at 6.5%. The cost of a healthcare breach, at \$282 per record, was more than twice as high as that of the average retail breach at \$131 per record. And the incentive to capture this information is compelling—in fact, medical ID theft has outstripped credit card theft as a moneymaking opportunity; while credit cards with card security codes (CVVs) fetch \$10-\$20, health records now fetch \$50 to \$60 each. Meanwhile, hackers are increasingly targeting healthcare and medical facilities. According to the San Diego-based nonprofit organization Identity Theft and Resource Center, healthcare was responsible for 20.5% of exposed records in 2008. This totals more than 7 million records, and is the second highest percentage, behind only the government/military sector. This is partly because this sector is an easy target with lax security controls, and partly because the rewards of breaking into healthcare systems are increasing as healthcare providers keep more records in electronic form.

Overall, the feeling is that while HITECH is not in itself a security or privacy rule, it may well drive the more stringent oversight and enforcement that HIPAA has been lacking. The significant amount of taxpayer dollars involved in the Act is almost certain to force more transparency and accountability. The mandatory notifications will motivate providers even further, by threatening not just a drop in incentive funding and HIPAA-related fines but a negative effect on their "brand."

How Your Network Can Help Prepare You for HITECH

Measurable Security

Many sections of the Interim Rule refer to HIPAA security and privacy rules; in fact, the first guidance document published by the Department of Health and Human Services deals specifically with steps that should be taken to protect ePHI. "All e-PHI created, received, maintained, or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of e-PHI. Risk analysis is the first step in that process" (excerpted from HIPAA Security Standards: Guidance on Risk Analysis). Another factor to consider is that the HITECH Act requires tracking of all ePHI disclosures. Such a task can become a nightmare if PHI is shared with hundreds of business partners, associates, and other third parties. Risk mitigation requires visibility.

A key tool in reducing risk is to have visibility on what is truly happening throughout your network, including when assets are being accessed off the medical campus. A comprehensive monitoring and reporting system is vital to give you the “aerial” view that you need. The right solution should correlate information from many different vendors’ products to give you a picture of the network as whole. Not only will this help you see what is happening in real time, such a tool can help to develop baselines and provide closed loop feedback on changes. More importantly, it automates a traditionally costly and time-consuming process of manually looking for a potential breach and only reacting to it after the fact. It also serves as a deterrent to potential malicious insiders, who might be reluctant to do something abusive if they knew they were being tracked.

Find out more about how Juniper Networks STRM Series Security Threat Response Managers can help by clicking here: www.juniper.net/us/en/products-services/security/strm-series/.

Increased Volume

The incentives of the HITECH Act, as well as the rapid pace of product development and the increased velocity of life critical healthcare applications going online, all promise that network traffic will escalate dramatically in the coming years. We will ask things of our networks for which they might very well not have originally been designed. This is particularly true given the variety of wireless devices, diagnostic and treatment equipment, patient facing applications, RFID tags, and telemetry equipment, which may not even be visible to most users. Thus, a key area of focus is the data center, many of which are built on antiquated, layered device models. Over the years, data centers have become bloated and complex. Each time a new system has come online, money has been thrown at the problem. This has resulted in more servers, more appliances, more gear, more complexity, and also more compliance risk.

The right solution to meet this challenge must be able to scale intelligently without sacrificing security. This can be accomplished through simplification of the data center both from an infrastructure and a security perspective. More is not better and the goal is to reduce the data center footprint, yet get more out of it. This can be accomplished by reducing the number of switches and layers in the traditional data center, which has grown bloated and inefficient over the years. With the latest switching technology, older switches can be reduced by a factor of ten, and new switches are also flexible enough to be deployed in a top-of-rack and/or end-of row configuration. This combined with collapsing the port and aggregation layers can reduce the overall footprint and make the data center more efficient, less complex, and less costly. Additionally, firewalls and gateways must be able to keep up, even with sophisticated services such as IPS and stateful packet inspection turned on. Both the infrastructure and the security in the data center should be capable of processing vast amounts of traffic, while flattening the overall architecture for easier maintenance and management.

Find out more about how Juniper’s New Network can help by clicking here: www.thenewnetworkishere.com/us/en/.

PCI DSS

The Really Big Stick

PCI DSS has been a game changing regulation in the financial and retail industries for almost a decade, but has not yet come up on the majority of healthcare organizations’ radar. Some experts believe that part of the issue is the fact that Medicare reimbursement is not at risk with PCI compliance, and that the regulations have therefore been largely ignored. However, that scene is set to change, and, as it does, some healthcare providers will find themselves at risk of significant fines.

What is PCI DSS?

The Payment Card Industry describes the PCI Data Security Standards as “...a set of comprehensive requirements for enhancing payment account data security.” PCI DSS was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. International. The goal was to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. Anyone who accepts a credit card as payment is referred to as a “merchant” in PCI parlance, and is subject to following PCI rules.

How is PCI DSS Different?

At the most basic level, HIPAA asks the healthcare organization to create and describe controls they have put in place to meet the goals of that standard. An auditor then evaluates whether the controls are effective, and finally weighs in on how well the organization is performing those controls. PCI DSS, on the other hand, spells out exactly what controls should be in place and how they should be implemented without subjectivity; auditors are concerned with whether these specific requirements have been implemented and are working. HIPAA is synchronized with PHI wherever it might be. PCI is concerned only with what the standard has described as the “PCI Zone;” a separate network zone or VLAN where cardholder information resides. A quick contrast of the two specifications includes the following points:

Table 2. HIPAA and PCI DSS Comparison

HIPAA	PCI DSS
United States federal law	Part of a contractual agreement between the major credit card brands and any merchant
Concerned with patient health information	Concerned with cardholder data
Quite flexible, using any security measure that reasonably and appropriately implements the requirements of the law	Extremely prescriptive, with detailed, specific information about security measures that must be employed in every area that cardholder data passes through
Organizations able to determine whether addressable specifications are reasonable, and may argue why they are not	PCI rules that are absolute and do not change merchant-to-merchant
Inconsistently enforced	Visa alone able to levy fines of up to \$500,000 per incident; In some cases merchants have been fined up to \$25,000 for non-compliance infractions

Table 3. PCI DSS Goals and Requirements

GOALS	PCI DSS REQUIREMENTS
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords & other security parameters
Protect Cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain and information security policy	12. Maintain a policy that addresses information security for employees and contractors

Please note that while this table seems easy to digest and quite compact, it is only a very superficial look at the goals and top line requirements of the statute. The full PCI DSS mandate includes literally hundreds of very detailed sub and sub-sub requirements, all of which need to be addressed.

The idea that providers are not storing credit card numbers and therefore need not be concerned with PCI DSS is a misinterpretation of the standard. PCI DSS is concerned with three primary aspects of card security: storing, processing, and transmitting. This means that if an organization—whether fundamentally retail, financial, healthcare, or other industry—processes a credit card, that organization must be PCI compliant. When viewed through the lens of PCI DSS, any organization

that accepts credit cards for payment is considered a merchant, regardless of industry. Each of the five major card brands designates its own version of “merchant level,” a requirement that mandates the level and frequency of audits and the type of audit required based on transaction volume and geographic location (among other factors). However, it is important to note that PCI compliance is still mandated, regardless of transactional volumes. As healthcare organizations continue to add new applications and services, it is likely that the number of transactions will increase, bringing providers further into the PCI spotlight.

Why aren't healthcare providers getting in front of PCI DSS? According to Forrester, the majority of healthcare IT budgets go to keeping existing systems running. “With scarce resources available, healthcare IT decision makers allocate, on average, 78% of IT operating budgets toward the maintenance of operations and ongoing IT software and hardware capabilities, leaving a mere 22% for new IT initiatives and projects. A further study shows that the healthcare industry allocates only 10.9% of the IT operating budget to security.

In fact, PCI DSS is generally perceived as one of the most difficult regulations with which to comply because it is so specific. In a recent analyst survey, 69% of respondents already compliant with PCI DSS ranked it as a difficult/very difficult regulation with which to comply; HITECH and HIPAA compliance were seen as significantly less arduous. It is important to note that the perception of difficulty skyrockets if respondents are not already compliant; in this case PCI DSS is seen as difficult/very difficult by a full 85% of noncompliant respondents, while the difficulty of complying with HITECH and HIPAA are virtually unchanged. Interestingly, the individual controls specified by the PCI DSS are not new or unique, or even overly difficult. PCI has focused on mature technologies and strategies to lower any barrier to compliance. What PCI does require, however, is a coordinated, consistent approach.

What about PCI DSS Enforcement?

One may wonder why healthcare organizations are not suffering from the burden of noncompliance with PCI DSS. The simple fact is that the card brands and the PCI Security Standards Council assume self enforcement. While this may seem disingenuous, consider the fact that complying with PCI DSS is part of the contract that merchants enter into with the card brands. As Forrester says, “Because PCI DSS compliance is part of a broader legal contract, companies using credit cards cannot just ignore PCI. It's not merely a best practice that you can choose to implement if you want to, nor is it a governmental regulation that may or may not be consistently enforced. This means that noncompliance is not an option. Noncompliance is penalized by fines, fees, and other costs. The card brands and acquirers have proven that they will enforce PCI DSS and penalize organizations where appropriate.”

How Your Network Can Help Prepare You for PCI DSS

Logging and Reporting

PCI DSS is devoted to getting a picture of the network as a whole, not a piecemeal look device by device. This capability is essential in meeting requirement 10, which mandates that you track and monitor all access to network resources and cardholder data.

An ideal way of meeting this requirement is an overall monitoring tool that can pull information from products throughout your network, regardless of vendor. This kind of tool gives you the true picture you need to meet compliance. Such a solution would also feature preconfigured reports to make it easy to create closed loop security, as well as to go through an audit. The right network monitoring system can also go a long way toward meeting HIPAA requirements, and provide the documentation required to survive audits as they occur.

Find out more about how Juniper Networks STRM Series Security Threat Response Managers can help by clicking here: www.juniper.net/us/en/products-services/security/strm-series/.

Granular Secure Access Regardless of Location

PCI DSS features several requirements designed to deliver secure access to authenticated, authorized individuals, regardless of their location. Requirement 4 of PCI DSS mandates that merchants encrypt transmission of cardholder and sensitive information across public networks. Requirement 8 mandates that organizations assign a unique ID to each person with computer access. According to Forrester, however, “healthcare companies primarily use only passwords to authenticate users (43% of remote access to intranet; 33% of business partners accessing extranet; 38% of customers performing online transactions),”

These requirements need to be met by a solution that combines secure remote access with strong network access control. Such a system should enable very granular permissions for remote users from any device, and then carry those access controls with the user as they change location, giving complete user mobility without sacrificing identity-based security. Such a system can ease the requirements of HIPAA as well, by providing secure access to users regardless of location (home, clinic, hospital) or device (desktop, laptop, smartphone), be it managed or unmanaged.

Find out more about how Juniper Networks SA Series SSL VPN Appliances can help with remote access security by clicking here: www.juniper.net/us/en/products-services/security/sa-series/.

Find out more about how Juniper Networks Unified Access Control can help by clicking here: www.juniper.net/us/en/products-services/security/uac/.

Firewalls and Intrusion Prevention

PCI DSS devotes an entire section to firewall setup and placement, as well as numerous other areas citing how the devices are to be deployed and configured. Zone-based security is stressed through the rule. While there are several places in PCI DSS where IPS are helpful, requirement 11.4 is probably the most direct. It states, "Use intrusion detection systems, and/or intrusion prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises." Unfortunately, many IPS systems are costly and difficult to manage, and using them can create performance bottlenecks, which is the last thing a healthcare organization can tolerate.

The right solution should feature an integrated approach, enabling the organization to take advantage of the functionality it requires without the need to rip and replace devices or invest in a costly "uni-tasker." Performance should be optimized to ensure that overall network throughput is maintained. Finally, a good solution should be capable of being tied into an overall logging and monitoring system, to enable early alerts, and to function seamlessly while also being able to proactively demonstrate compliance to the regulatory body. This closed loop functionality enables the provider to meet many requirements posed by PCI DSS, giving the baseline information required to determine and thwart future threats as well as to get to the bottom of existing problems.

Find out more about how Juniper Networks SRX Series Security Services Gateways can help by clicking here: www.juniper.net/us/en/products-services/security/srx-series/.

Conclusion

When considering compliance, today's healthcare organization is faced with enormous challenges. However it is important to realize that there are significant benefits to compliance as well. In the past, efforts by the IT or security teams to implement proactive controls may have fallen on deaf ears, as many CFOs have been largely concerned with just keeping the myriad of separate systems running day to day. But today, such projects are easier to justify. HITECH brings the promise of ePHI funding which will create a truly competitive advantage for institutions. The need for PCI DSS compliance can make security into an excellent investment, particularly when compared to the costs of noncompliance.

In order to help meet compliance requirements, healthcare organizations need a network that is:

- From a proven leader well versed in today's challenges and potential solutions that healthcare organizations can use to solve them.
- Deployed as a platform for innovation (we all know the compliance standards today; the challenge is to be able to quickly and comprehensively address new legislation and new requirements without having to start over from scratch)
- Based on open standards to ensure interoperability and promote a best-in-class approach without getting locked into any specific vendor
- Greater than the sum of its parts, providing services that work ubiquitously, and can provide comprehensive, proactive security and compliance without negatively impacting mission critical operations or breaking the bank

By meeting these goals, the healthcare organization can seamlessly and proactively meet a variety of dynamic and complex regulations, both today and tomorrow, while ensuring the security they need to provide quality care for their patients and serve their communities.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

- ⁱ Forrester. Healthcare Security: Ready or Not, Here It Comes , July 24, 2009.
- ⁱⁱ Gartner. Addressing HIPAA Security, Part 2: 'Rightsizing' Compliance, September 23, 2009.
- ⁱⁱⁱ Gartner. Addressing HIPAA Security, Part 1: The Standards, September 23, 2009.
- ^{iv} Forrester. Healthcare Security: Ready or Not, Here It Comes , July 24, 2009.
- ^v Forrester. Demand Insights: Healthcare Budgets and Spending Trends.
- ^{vi} Ponemon. The State of Privacy and Data Security Compliance, November 20, 2009.
- ^{vii} Forrester. PCI Unleashed, January 11, 2010.
- ^{viii} Forrester. Enterprise and SMB Security Survey; North America and Europe, Q3, 2008.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

2000162-001-EN Aug 2010

 Printed on recycled paper

