Latest Changes in Healthcare Regulations—and the IT Solutions Needed to Address Them

Five critical IT capabilities providers need to stay in front of today’s evolving regulatory environment

Table of Contents

Executive Summary

Over the past decade, it is likely that no industry has undergone as much rapid, controversial, and dramatic change as the healthcare industry—and the changes keep coming. Even as the system as a whole undergoes its most significant reform in decades, the regulatory environment is also stiffening, which is escalating the pressure on healthcare organizations to enhance their security and privacy measures, even as they deal with the proliferation of mobile devices and other technological challenges. There is much at stake, and because virtually all security and privacy regulations are enabled by or dependent on technology, IT will play a major role helping the industry address its significant security and privacy challenges. At the same time, there is also an opportunity for healthcare organizations to create a competitive advantage through investing in superior IT solutions.

Introduction

The latest change to the regulatory environment is the omnibus rule that went into effect in March 2013. The new rule enhances the Health Insurance Portability and Accountability Act (HIPAA) of 1996, increasing patient privacy protections, adding more individual rights to health information, and strengthening government enforcement of HIPAA privacy and security protections, with broader breach discovery, much larger fines, and even the possibility of jail time for noncompliance.

Recent court cases and fines provide a convenient reminder of the cost of ignoring or overlooking the latest omnibus rule. Consider these 2013 cases alone:

- Advocate Health Care: Four unencrypted laptops were stolen from an Advocate Health Care facility in Illinois. The theft compromised the protected health information and Social Security numbers of more than 4 million people and has led to a class-action lawsuit by affected patients.
- Affinity Health Plan: The organization sold a photocopier that contained confidential medical information on the hard drive, affecting more than 344,000 individuals and leading to a $1.2 million settlement.
- Allied Health System: A medical assistant inappropriately viewed the electronic health records of nearly 4,000 patients over a three-year period. The breach, which was reported in September 2013 and may have affected patients across 11 hospitals and 50 physician clinics, was the 682nd patient data breach in the U.S. since 2009.

Given the rapid evolution of the regulatory environment and the soaring penalties for noncompliance, it is vital for healthcare organizations to adopt advanced IT solutions that enhance security and privacy protections in a comprehensive, timely, and cost-effective manner. Specifically, healthcare organizations need to address five critical IT capabilities: security management, protection of IT infrastructure, applications, data access, and endpoints.

The Ponemon Institute's Third Annual Benchmark Study on Patient Privacy and Data Security, conducted in December 2012, found that:

- 94% of healthcare organizations studied had at least one data breach in the past two years; 45% had more than five.
- The average economic impact of data breaches over the past two years was $2.4 million—an increase of $400,000 since 2010.
- 57% of data breaches cost more than $500,000, an increase of nine percentage points since 2010.
- 52% of organizations reported one or more incidents of medical identity theft.
- 62% of healthcare organizations make moderate or heavy use of cloud services; however, 70% percent are not or only somewhat confident that information in the cloud is secure.
- 40% of healthcare organizations have confidence that they can prevent and detect all patient data loss or theft in their organizations.

Omnibus Rule Increases Requirements, Creates New Challenges

When first enacted in 1996, HIPAA was roundly criticized for lacking sufficient "bite." The lack of adequate incentives, penalties, and enforcement, as well as the vagueness of HIPAA guidelines, led to widespread industry and public complaints.

Those early criticisms help explain what has occurred since, most recently with passage in January 2013 of the final omnibus rule, which Leon Rodriguez, director of the Office for Civil Rights (OCR) of the Department of Health and Human Services, says contains "the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented."

The new omnibus regulations institute the following three key changes to HIPAA:

- Expand the obligations of physicians and other healthcare providers to protect patients' protected health information (PHI)
- Extend those obligations to other individuals and companies that are "business associates" with access to PHI
- Increase the penalties for violating the above obligations

The new omnibus rule has taken the increased security standards that became law under the Health Information Technology for Economic and Clinical Health (HITECH) Act and moved them under HIPAA. One result is that the HITECH Act's Breach Notification requirements have been expanded and clarified. Previously, breaches of unsecured health information had to be reported when they met the legal standard of "risk of harm"; now, the standard has been lowered, meaning healthcare organizations will likely need to report more breaches.

Another change under the new omnibus rule—namely, the expansion of many existing HIPAA requirements to business associates—affects contractors, subcontractors, and even cloud providers and other vendors that never view or interact with PHI. Some of the largest breaches reported to the U.S. Department of Health and Human Services have involved business associates, and the omnibus rule makes it likely that more such cases will occur in the future.

Penalties for noncompliance are also greater than ever under the new rule, even as the challenge of protecting patient privacy increases. The maximum penalty is $1.5 million per violation, with the amount based on four tiers, ranging from cases in which physicians do not and could not reasonably know of the breach to those in which physicians act with willful neglect that is uncorrected.

Related Challenges

The final omnibus rule has received a great deal of attention, but to be clear, it is just one of many security and privacy challenges facing today's healthcare organizations. The growing use of unsecured mobile devices, the rise of unintentional employee mistakes, the emergence of Payment Card Industry Data Security Standard (PCI DSS) issues, the increased professionalism of attackers—not to mention shrinking IT budgets—are all contributing to one of the most challenging periods in the history of U.S. healthcare.

A single solution to all these issues does not exist, but most of the challenges point to the need for more sophisticated, scalable, and adaptive IT solutions. That's because virtually all security and privacy regulations are enabled by or dependent upon technology and its ability to ensure the confidentiality, integrity, and availability of information assets that are used by healthcare organizations and their extended ecosystem of partners, suppliers, and customers.

Five Critical IT Capabilities to Help With New Regulations

Only by upgrading the IT solutions that underpin privacy and security can healthcare organizations optimize their business operations while also preventing costly data breaches and complying with the new omnibus rule and other regulations.

Specifically, organizations must have adaptive threat management solutions in place that focus on five critical areas:

1. Security management
2. Infrastructure
3. Applications
4. Access to data
5. Endpoints

Provide Reliable Security Management

Growth in network traffic, including mobile traffic, as well as the emergence of cloud services and the increasing sophistication of malicious hackers have made it increasingly difficult, costly, and complex to manage enterprise security policy. Today's security management is often error-prone and time-consuming, especially when management solutions are difficult to use or restricted in the granularity of control. Resulting misconfigurations can leave healthcare organizations vulnerable to attacks and noncompliant with regulations and policies.

Better security and compliance must begin at the top, with IT solutions that provide control, visibility, and response across the entire IT landscape. A comprehensive view of all security-related activity is particularly necessary given the new omnibus rule, which places more pressure on healthcare organizations to recognize and report more data breaches and be aware of which business associates (vendors, subcontractors, etc.) have access to PHI.

Security management solutions need to provide comprehensive management and control of all security-related applications, devices, and infrastructure, with simplified operations across multiple device types. From one centralized, web-based interface, administrators should be able to report on all phases of their security policy lifecycle quickly and intuitively.

Find out more about Juniper's security management solutions, including Juniper Networks® JSA Series Secure Analytics (formerly known as STRM Series Security Threat Response Managers) and Junos® Space Security Director, at www.juniper.net/us/en/products-services/security.

Protect the Data Center

Protecting the infrastructure—including network, servers, and storage—has always been at the top of the to-do list for IT administrators. The difference now is that the challenges, and penalties for failure, are greater. Attackers are more organized and sophisticated, and the technology itself is more complex, with traditional and virtualized workloads vulnerable to wrongful access, breaches, and other exploits.

Ideally, healthcare organizations need a range of protection that spans enterprise core, edge, and branch, all from a single product line, which helps ensure consistent policy enforcement throughout the transaction ecosystem. Next-generation firewall capabilities should be comprehensive, with stateful firewall, intrusion protection, and application visibility and control.

Infrastructure solutions also need to be flexible enough to work on both traditional and virtual servers. Security needs to go beyond the hypervisor level to wrap around virtual machines, ensuring better throughput without sacrificing security. Solutions should also be able to scale incrementally, without having to shut down and disrupt end users.

Find out more about Juniper's infrastructure protection solutions, including the Juniper Networks SRX Series Services Gateways and the vGW Virtual Gateway, at www.juniper.net/us/en/solutions/enterprise/security/platforms.

Provide Advanced Application Protection

Applications, and particularly Web applications, are one of the most targeted areas for exploitation, especially in today's increasingly distributed IT environments. Because many apps are built by people who lack knowledge of proper security measures, and are not known or monitored by the IT department, they are particularly vulnerable to attack.

Fortunately, advanced application protections are emerging to help reduce the number of application-based breaches, prevent known attackers from coming back, and lower the risk of internal users accidentally introducing malware. By implementing these advanced protections, healthcare organizations can also reduce the likelihood of hefty fines under HIPAA and the new omnibus rule.

The best application protections identify attackers' behavior early on, engage them so they believe that they are effectively breaking in, and then fingerprint their devices so they will be detected when they try to hack the next Web app. This so-called "intrusion deception" changes the economics of attacks because hackers are fooled into spending a lot of time without getting results and are therefore less likely to continue trying to attack the organization.

Find out more about Juniper's application protection solutions, including Juniper Networks Junos AppSecure, Junos Spotlight Secure, and Junos WebApp Secure, at www.juniper.net/us/en/solutions/enterprise/security/applications-content.

Control Data Access

Access control is critical for any enterprise, but especially for healthcare organizations because of the large amount of vulnerable PHI and the need to balance security, convenience, and privacy across numerous user types. To complicate matters further, the new omnibus rule extends privacy and security obligations to a wider array of business associates, placing a greater onus on organizations to have extremely high levels of visibility and control over data access.

Access control solutions should provide context-aware security and truly granular access policy controls for all devices across a global network. For ease of use and flexibility, the solutions need to accommodate both remote and onsite workers, and adapt depending on conditions such as data type. To increase productivity, secure, consistent access should also be ensured regardless of device, based on identity, device type, and location.

Healthcare organizations should also look for open, standards-based network access control, which will help lower costs and ease deployment and integration by enabling use of third-party network and security devices. Organizations can also lower costs and speed deployment with access control solutions that are vendor-agnostic.

Find out more about Juniper's access control solutions, including Juniper Networks Junos Pulse Access Control Service and Junos Pulse Secure Access Service (SSL VPN), at **www.juniper.net/us/en/solutions/enterprise/security/connectivity**.

Defend Endpoints

Healthcare organizations need to be able to easily and securely connect many different types of users (remote, mobile, patients, partners, vendors, etc.) to networks, applications, and data, based on dynamic security policies. Doing so reduces the risks of endpoint data breaches, as well as mobile application exploits.

While securing endpoints (users and devices) is an essential part of overall security and HIPAA compliance, it is also necessary to provide end users with consistent, reliable connectivity and remote access to organizational resources. The connection process needs to be simple, fast, and easy to use, as well as safe. On the IT side, network and application access should be location-aware, identity-enabled, and federated across myriad platforms.

An SSL VPN can be used to secure connectivity across all user devices, which helps simplify mobile security management. Network access control at the device and session level is also needed for remote, onsite, and guest users—including the business associates that are now more closely monitored under the new omnibus rule.

Find out more about Juniper's endpoint security solutions, including Junos Pulse Client, Junos Pulse Mobile Security Suite, Junos Pulse Secure Access Service (SSL VPN), and Junos Pulse Access Control Service, at www.juniper.net/us/en/products-services/software/junos-platform/junos-pulse.

Conclusion

Achieving compliance with the new omnibus rule and other emerging privacy and security regulations is a growing challenge for healthcare organizations. However, it is important to realize that there are significant benefits to compliance—not just in avoiding penalties but in implementing superior IT solutions that will help organizations scale faster, run more efficiently, and be more productive.

In the past, efforts by IT and security teams to implement proactive controls may have fallen on deaf ears, as many CFOs were largely concerned with keeping systems running from day to day. But today, more executives recognize that such measures are essential because of greater enforcement, broader breach discovery, increasingly costly penalties, and the threat of jail time. Executives are also more likely to recognize the opportunity to establish competitive advantage through investing in superior IT solutions.

To help meet emerging HIPAA compliance requirements, healthcare organizations need adaptive threat management solutions that are:

- From a proven leader, well versed in today's challenges and the solutions healthcare organizations can use to solve them
- Deployed as a platform for innovation, so that organizations can quickly and comprehensively address new legislation and new requirements
- 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 their parts, providing cost-effective services that work ubiquitously and can provide comprehensive, proactive security and compliance without negatively impacting mission-critical operations

By focusing on these goals, healthcare organizations can seamlessly and proactively meet a variety of dynamic and complex regulations, both today and into the future.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

2000545-001-EN Sept 2015