



Internet Filtering: Meeting the Challenge of HIPAA Compliance

INTRODUCTION

Acting fast under pressure is business as usual for many companies in the healthcare industry. But behind the scenes, hospitals, insurance providers, and other organizations are racing to meet a different kind of challenge: Complying with new federal security regulations set out in the Health Insurance Portability and Accountability Act (HIPAA).

Specifically, the new rules stipulate the measures healthcare organizations must take to safeguard protected health information (PHI), and they set April 2005 as the date for having those measures in place. The deadline is even more demanding given the scope of the work involved: Ensuring proper handling and preserving the confidentiality of PHI requires healthcare organizations to implement a strategic security initiative covering a range of potential vulnerabilities and liabilities.

Web content filtering plays a vital role in meeting the challenges of HIPAA compliance, and M86 Security is helping healthcare organizations on this front with its R3000 Enterprise Filter. The R3000 is a flexible, highly scalable network appliance that can be deployed to limit improper access to PHI and preserve its confidentiality, directly addressing the main provision of the HIPAA rules. It also comes with comprehensive tracking and reporting capabilities that can assist in demonstrating compliance—and in ensuring the trust of patients and partners alike. And thanks to simple setup and an open-source OS, the R3000 can be quickly and easily implemented as an integral part of a healthcare organization's overall approach to meeting the new HIPAA guidelines.

Web content filtering plays a vital role in meeting the challenges of HIPAA compliance, and M86 is helping healthcare organizations on this front with its R3000 Enterprise Filter.

HIPAA: THE FACT SHEET

HIPAA was enacted in 1996, and much of it addresses the issue of portability—that is, the continuity of healthcare coverage as individuals change jobs or careers. But HIPAA also sets out detailed regulations on the confidentiality of patient records and keeping them safe from unauthorized use or viewing, and that's what healthcare organizations have to be most concerned about.

Given the electronic nature of most PHI, from insurance approvals to prescription requests to medical histories, the implications for the industry are enormous. Mishandling confidential data not only raises the likelihood of civil and criminal penalties; it also could result in the loss of an organization's reputation, credibility, and customers.

In an effort to meet regulations and limit their liability, healthcare organizations have to view compliance in the context of their overall business. The importance of this approach is made clear by the scope of the HIPAA rules. They cover all entities equally, regardless of size or structure; they are comprehensive, stipulating a uniform system of PHI safeguards; and they are technology-neutral, providing little in the way of guidance beyond suggesting that companies select and deploy the tools they deem most helpful.

All of that makes it incumbent on CTOs, CIOs, and other information technology professionals to work closely with senior executives in devising a PHI security strategy. It should take into account the risks to the organization, and their relative priority to one another; the steps that need to be taken to reduce risk and ensure HIPAA compliance; and the cost—in terms of money, labor, technology, and other resources—to ensure compliance.

With a strategic plan in place, healthcare organizations are in a much stronger position to tackle the specific security requirements set out in HIPAA. Among the most important:

- Ensuring the confidentiality, integrity, and availability of all PHI the covered entity creates, receives, maintains, or transmits
- Protecting against reasonably anticipated threats or hazards to PHI
- Protecting against reasonably anticipated uses or disclosures of PHI as defined in the HIPAA guidelines
- Implementing procedures to determine whether individual employee access to PHI is appropriate
- Implementing procedures for guarding against, detecting, and reporting malicious software
- Implementing procedures to record information system activity and regularly review those records
- Ensuring a flexible but comprehensive and effective approach to safeguarding PHI

HIPAA was enacted in 1996, and much of it addresses the issue of portability—that is, the continuity of healthcare coverage as individuals change jobs or careers.

DANGEROUS BEHAVIORS

When it comes to protecting the integrity of confidential and mission-critical data, hospitals, pharmaceutical companies, insurance providers, and other healthcare organizations face many of the same challenges companies in other industries do. While they have to be on constant guard against unwanted incursions from the outside, they must also simultaneously keep their own employees from (unwittingly or wittingly) doing damage from the inside.

And the unfortunate fact is that healthcare employees are no less prone to the missteps and misbehavior of their brethren in other sectors. They visit unauthorized Web sites on company time. They use Web-based e-mail and instant messaging (IM) to communicate with friends and other outsiders. They take advantage of peer-to-peer (P2P) and file-sharing technology to trade music and download movies. And by engaging in this activity they all put PHI at greater risk—even if unintentionally.

How? The sites that employees choose to visit may contain spyware, adware, and malicious code, all of which can compromise the integrity of systems and data. Web-based e-mail applications like Yahoo and Hotmail aren't subject to the restrictive security policies governing corporate applications, so there's no way to block errant transmissions of sensitive information. P2P sites like Morpheus can open the corporate network to the world by opening a backdoor through which anyone can peek into devices and the data stored on them.

Of course, there are also those employees who either purposely put data at risk or play a more active role in compromising its integrity. They might use unguarded Web-based e-mail to share unauthorized information on a new drug. They might IM their friends with details of a patient's hospitalization. Or they might use those applications in seeking to capitalize on their access to confidential information — whether it's details of a patent-pending technique or the private records of a famous patient (tabloids have been known to IM hospital personnel in search of celebrity scoops).

All of this would be bad enough if it didn't mean running afoul of federal regulations in the process. But HIPAA raises the stakes—and subjects healthcare organizations to penalties that companies in other industries don't have to face.

The sites that employees choose to visit may contain spyware, adware, and malicious code, all of which can compromise the integrity of systems and data.

THE ROLE OF WEB FILTERING

Fortunately, Web filtering technology can be used to address many of these potential vulnerabilities. Appropriately deployed, it can give healthcare organizations much greater control over access to sites, systems, and data—helping them preserve the integrity of their PHI, limit their liability, and comply with many of the specific security rules set out in HIPAA.

That's where the R3000 Enterprise Filter from M86 comes in. It's a flexible, highly scalable network appliance that not only features a range of filtering and reporting capabilities, but that also can be deployed quickly and easily to help healthcare companies safeguard PHI and demonstrate HIPAA compliance.

The R3000 sits at the gateway or aggregation point of the network, where it makes use of deep packet inspection to scan all internal traffic heading out to the Web. When it spots a violating packet—whether it's a request for a pornographic site, a Web-based e-mail application, or Internet radio/TV—it takes fast action on two fronts. First, it sends a block page to the workstation that generated the request, typically within 2 to 4 ms. Then it sends a TCP reset to the site to cancel the session. By sealing off access to unauthorized sites so quickly, the R3000 prevents confidential information from leaving the premises while simultaneously securing the network from unauthorized intrusion and malicious code.

But recent enhancements to the R3000 make it even better suited to healthcare organizations struggling with HIPAA compliance. It now features IM blocking, so that an organization's information and infrastructure won't be put at risk by employees who should be working rather than chatting. As with URL filtering, this can help limit legal liability, since employees who can't IM can't use it to transmit sensitive data. IM blocking also reduces the risk of virus infiltration. And in the M86 implementation, it serves as a baseline for P2P blocking—so that companies are protected against backdoor breaches from file-sharing sites.

The R3000 also comes with enhanced capabilities for blocking file download by type or extension, thanks to generic keyword filtering. Healthcare organizations are thus better able to build a wall against executables, RealAudio, and other files that might harbor malicious code.

Time-based filtering is another new feature. This allows administrators to permit or deny access to Internet resources during specified times, giving companies an even greater degree of control over users' online behavior. And with an expanded database library supporting more than 75 categories (from "alcohol" and "games" to "pornography" and "weapons"), the R3000 furnishes an accurate and selective solution for filtering and monitoring.

All of those features can help healthcare organizations directly address the security rules set out in HIPAA. But the R3000 also enables companies to meet guidelines mandating procedures for reviewing system activity—and thus demonstrate compliance in addition to achieving it.

That's because the R3000 is matched with the industry's leading reporting appliance, M86's Enterprise Reporter. It can investigate a company's Internet traffic down to the IP address; by typing in a user ID, an administrator can immediately retrieve the user history and drill down deep into specific details for a full picture of activity. This is a big advantage over canned reports that look only at high-level data.

And, armed with this kind of specific information, companies can locate the violator much more quickly, shaving valuable time off the investigative process—while offering even greater proof to regulators and partners alike that they are in compliance.

Given the complexities and challenges of adhering to HIPAA security rules, the last thing healthcare organizations need is technology that's inflexible, that doesn't scale, or that takes a bite out of productivity and performance. But the R3000 comes with a range of features that should give them peace of mind. First, it's based on Red Hat Linux. That not only makes for a stable and resource-efficient platform. It also puts companies in position to take advantage of all that open-source has to offer—from improved global support, to industry-standard technology advancements like gigabit Ethernet, to interoperability with a wide range of devices.

Second, it can scale to meet the needs of a growing business. The R3000 scales to 20,000 users per box; with authentication enabled, it can support up to 30,000 user connections at a 30-connection-per-second build rate.

Third, the R3000 is easy to set up and run. The software is pre-installed, so it can be put to work right out of the box. A new Java-based GUI features more intuitive navigation, making it even easier for administrators to define parameters and user groups. It ties in to customers' existing directory services, whether LDAP, Active Directory, or NT. And an online help feature keeps customers close to the information they need to optimize operation. All together, it adds up to easier administration and improved productivity.

Fourth, the R3000 runs in "invisible mode." It's not proxy-based but sits on the network, where it inspects packets without stopping them to do so. In other words, the R3000 adds zero latency—thoroughly assessing Web-bound traffic without incurring a penalty in performance.

When the real focus has to remain on protecting PHI, those features offer added comfort. Freed from worrying about configuration, administrative, and performance issues, healthcare organizations can instead concentrate on meeting the compliance guidelines that HIPAA defines.

CONCLUSION

Strict rules set out in HIPAA for handling PHI are putting new demands on healthcare organizations. Failure to secure patient data and protect it from unauthorized viewing or use presents considerable risk, in the form of civil and criminal penalties, increased liability, and loss of trust and reputation among customers and partners.

As part of an overall strategy for safeguarding PHI and achieving HIPAA compliance, healthcare organizations should implement Web filtering technology. It addresses many of the specific rules defined in HIPAA—from ensuring the confidentiality, integrity, and availability of PHI; to guarding against, detecting, and reporting malicious software; to recording information system activity and providing regular reviews of those records.

The R3000 Enterprise Filter is a comprehensive, cutting-edge solution for healthcare organizations facing the pressures of HIPAA compliance. It features a range of filtering parameters and blocking technologies to prevent access to unauthorized sites, transmission of sensitive information over Web-based e-mail and IM, and downloading of files containing malicious code. It also comes with advanced tracking and reporting capabilities to give healthcare organizations a detailed view of system activity—and a way to demonstrate compliance to regulators, partners, and customers. Scalability, simple setup, and an open-source operating system all help to ease administration and configuration, while performance is never an issue.

That's what makes M86's R3000 Enterprise Filter the correct choice for healthcare organizations facing the HIPAA compliance challenge. By deploying it as part of an overall strategy for ensuring the integrity of PHI, they can be sure to remain on the right side of new regulations.

ABOUT M86 SECURITY

M86 Security is a global provider of Web and messaging security products, delivering comprehensive protection to more than 20,000 customers and over 16 million users worldwide. As one of the largest independent internet security companies, we have the expertise, product breadth and technology to protect organizations from both current and emerging threats. Our appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers' networks from malware and spam; protect their sensitive information; and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit www.m86security.com.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters
828 West Taft Avenue
Orange, CA 92865
United States

Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters
Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Asia-Pacific
Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Auckland, New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 09.01.09