

# How NETGEAR® ProSecure™ UTM and STM Help Health Care Organizations Meet HIPAA Requirements

If you have visited a doctor's office in the last decade, you have likely signed a piece of legal-looking paper. It explained how your medical information might be used and disclosed and how you could get access to your information. This notification originated in 1996 with the Health Insurance Portability and Accountability Act (HIPAA), created to promote and regulate use of electronic health records.

As part of promoting its use, legislators wanted to ensure protected health information (PHI) would be used with care, shared only where justified, and secured against inadvertent exposure, loss, or theft. HIPAA outlined two sets of rules, the Privacy Rule and the Security Rule.

- The Privacy Rule governs how and by whom this sensitive information can be used
- The Security Rule protects the privacy of the information, while allowing adoption of new technologies to improve the quality and efficiency of health care

Where the Privacy Rule affects paper and oral information, as well as electronic information, the Security Rule only applies to electronic PHI (E PHI). This primer concentrates on the Security Rule, explaining HIPAA requirements in the context of the functions of the NETGEAR ProSecure UTM (Unified Threat Management) and ProSecure STM appliances. Start with HIPAA security, and you lay the technical foundation for HIPAA privacy.

## HITECH Act Stiffens Requirements and Boosts Penalties to \$1.5 Million

The original HIPAA legislation lacked major penalties or enforcement. It was also rather vague, so many health care organizations paid it little heed, especially smaller businesses that had limited IT expertise. Now, however, HIPAA merits careful attention. The American Recovery and Reinvestment Act of 2009 included the Health Information Technology for Economic and Clinical Health (HITECH) Act, which boosted the initially modest HIPAA penalties of \$100 per incident to "tiered ranges of increasing minimum penalty amounts, **with a maximum penalty of \$1.5 million** for all violations of an identical provision. A covered entity can no longer bar the imposition of a civil money penalty for an unknown violation unless it corrects the violation within 30 days of discovery."<sup>1</sup>

In addition to eliminating a loophole that allowed health care providers to plead ignorance of the rules, the Act also clarified some specific technical requirements, including use of encryption for data at rest and data in motion, and extended HIPAA requirements and penalties to include business associates of covered entities.

Finally, the HITECH act instituted notification to affected individuals of any breaches of unsecured protected health information. Patients expect health care providers to protect personal health information as carefully as they protect each patient's health. The disclosures now required by the HITECH Act mandate that covered entities reveal breaches of unsecured—usually unencrypted—PHI within 60 days. A revelation like that is expensive, from the damage it does to customer trust to the remediation effort and penalties required.

### Noncompliance can cost you

July 1, 2010—HealthNet agreed to pay a \$250,000 cash penalty on top of the over \$7 million it has spent because of a lost unencrypted drive with 27 million personal health records on it.<sup>2</sup>

## HIPAA "Covered Entities" Include Health Care Providers and Their Business Associates

Covered entities—health care providers, health plans, clearinghouses, and their business associates—have clear marching orders and motivations to respect and protect sensitive patient records and health information. Covered entities that contract with third parties must be clear that these third party business associates may also be subject to HIPAA controls.

- If your company assists health care providers by performing medical billing or other services involving protected health information, HIPAA requirements affect you.
- If you transmit protected health information electronically, HIPAA affects you.

---

1 <http://www.hhs.gov/news/press/2009pres/10/20091030a.html>

2. <http://www.infolawgroup.com/2010/07/articles/hitech-1/health-net-agrees-to-250000-fine-and-corrective-action-plan-to-settle-loss-of-phi/>

## Three Types of HIPAA Security Rule Requirements

The HIPAA requirements are broken into administrative, physical, and technical safeguards:

- **Administrative safeguards** manage the selection and execution of security measures to protect data. For example, one rule requires protective security measures to guard against, detect, and report malicious software (164.308.5.ii.b). Other activities might include formal termination procedures, where access privileges and passwords change when an employee resigns, or security incident procedures to ensure a quick response after a breach.
- **Physical safeguards** are the traditional “fences, locks, and dogs” of security. They protect computers, buildings, and other equipment from fire, environmental hazards, and physical intrusion.
- **Technical safeguards** protect, control, and monitor information access, through techniques such as access control, unique user identification, automatic logoff, encryption and decryption, audit controls, transmission security, authentication, and integrity controls.

HIPAA rules do not usually dictate specific technologies or vendors, instead offering guidance about the goals of each requirement. One solution can meet multiple requirements, multiple solutions can meet the same requirement, and some requirements can be met with compensating controls (a different security process or technology that achieves the same goal). No single technology can guarantee an organization will achieve HIPAA compliance. However, deploying multiple security layers will help. Covered entities are expected to take appropriate action based on the EPHI risks of their individual businesses.<sup>3</sup>

## Tackling HIPAA Compliance

One efficient way “covered entities” meet multiple HIPAA Security Rule requirements is by exchanging basic firewalls or network routers for unified threat management (UTM) appliances. Alternatively, one can install a content security appliance behind your existing firewall or router. Sitting at your gateway, your connection to the Internet, security appliances like these can help you comply with both administrative and technical safeguards through a combination of advanced malware protection and access, audit, authentication, and integrity controls.

Security appliances protect against external threats while increasing control over risky actions by employees. With an appliance, multiple security functions can be purchased in a convenient package and installed quickly and easily, for minimal disruption, with minimal expertise required. These products offer a variety of beneficial security and usage controls, such as:

- **URL Filtering**—Allows you to control the websites users can access to ensure compliance with policies and restrict undesirable activities
- **Anti-spam**—Blocks or quarantines nuisance and risky email that can carry data-stealing malware, enable phishing, clog email servers, and tax network bandwidth
- **Anti-malware**—Scans content looking for malicious code such as spyware, viruses, and Trojans
- **Application Control**—Allows you to enforce network usage policies and preserve productivity by blocking access to public instant messaging and peer-to-peer applications

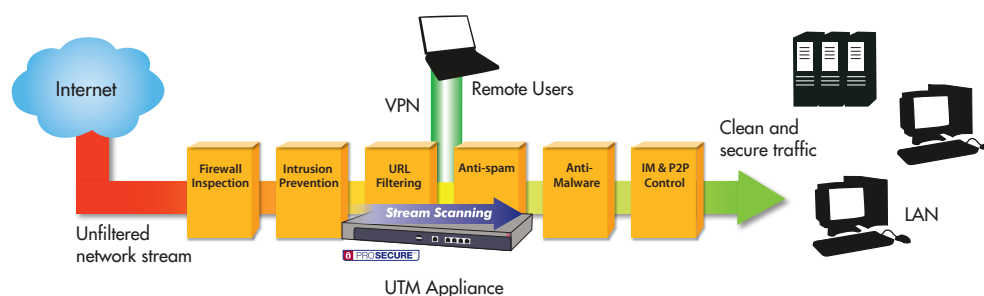


Figure 1: Multi-function Appliances Help You Comply with HIPAA Requirements While Implementing Higher Levels of Security Against Internet Threats.

- **Firewall Inspection**—Applies rules to network traffic to block or allow access to your network, limiting the risk of denial-of-service attacks and unwanted access to internal resources
- **Virtual Private Network (VPN)**—Allows safe remote access to your network by approved users, encrypting transmissions to protect traffic
- **Intrusion Prevention**—Inspects network traffic looking for unusual activity, zero-day threats, hacking indications, and risky content, and drops traffic that it believes is dangerous

<sup>3</sup> The US Department of Health and Human Services provides tools and guidance for download at <http://www.cms.gov/HIPAAGenInfo/>

These capabilities block threats from the outside that might jeopardize compliance, such as malware on websites and in email, hackers trying to break into your systems, and zero-day exploits (threats that take advantage of weaknesses in browsers, applications, and operating systems).

Encryption ensures that data you transmit over the network cannot be read or changed, and is an explicit requirement of HIPAA compliance. A VPN allows employees to securely access data and applications from their homes or other sites.

In addition, you can manage and restrict Internet use by your employees and guest users. These controls can enhance employee productivity while decreasing the chance of deliberate or accidental exposure of protected health information. You can pick a level of control from tight lockdown—blocking all sites other than those needed for business operation—to simple filtering of inappropriate content such as adult, gaming, and social media websites.

## Core HIPAA Requirements and ProSecure UTM/STM

The chart below shows the specific HIPAA safeguards addressed by the NETGEAR® ProSecure™ UTM Firewall and STM content security appliances. For simplicity, we have matched ProSecure functions to the recommendations in a white paper available from the U.S. Department of Health & Human Services website.<sup>4</sup>

Standards	Sections	Implementation Specifications	How NETGEAR ProSecure helps
<b>Administrative Safeguards</b>			
Security Awareness and Training	164.308(a)(5)(ii)(B)	Protection from Malicious Software	<ul style="list-style-type: none"> <li>Scans web and email traffic to remove malicious software</li> <li>Logs and reports malware incidents for speedy cleanup</li> <li>Hourly automatic malware signature updates ensure protection against the latest known threats</li> <li>Zero-day detection stops previously unknown threats without the need for the latest malware signatures</li> </ul>
	164.308(a)(5)(ii)(C)	Log-in Monitoring	<ul style="list-style-type: none"> <li>Captures log-in attempts on the management interface so you can identify suspicious activities</li> </ul>
Security Incident Procedures	164.308(a)(6)(ii)	Response and Reporting	<ul style="list-style-type: none"> <li>Logs and reports security incidents and violations to help you identify and remedy issues</li> </ul>
<b>Technical Safeguards</b>			
Access Control	164.312(a)(1)	Unique User Identification	<p>UTM and STM:</p> <ul style="list-style-type: none"> <li>To prevent unapproved changes or malicious access, management can be limited to a list of approved users called an ACL (access control list)</li> <li>Allows or blocks incoming/outgoing web and email traffic based on policies</li> <li>Authenticates users to allow appropriate role-based web access</li> </ul> <p>UTM Only:</p> <ul style="list-style-type: none"> <li>The firewall prevents unwanted network access from the outside</li> <li>Intrusion prevention blocks hacking and system attacks</li> <li>SSL and IPSec VPNs allow secure remote access</li> <li>Authenticates users to confirm legitimate access to VPNs and websites, leveraging existing user directories (LDAP, RADIUS, Active Directory)</li> <li>By defining separate network segments for internal (VLAN) and guest (DMZ) traffic zones, you can limit access to EPHI while allowing guests to access the Internet</li> </ul>
		Automatic Logoff	<ul style="list-style-type: none"> <li>UTM/STM administrators are automatically logged off after a period of inactivity to limit the chance of unauthorized use</li> </ul>
		Encryption and Decryption	<ul style="list-style-type: none"> <li>VPN traffic through the UTM is encrypted and decrypted using industry-standard algorithms such as DES, 3DES, AES (128, 192, 256 bit), SHA-1, and MD5</li> </ul>

<sup>4</sup> Download your copy from <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf>. A more detailed paper is available from the National Institute of Standards and Technology (NIST) website: <http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>

Standards	Sections	Implementation Specifications	How NETGEAR ProSecure helps
Audit Controls	164.312(b)		<ul style="list-style-type: none"> <li>Supports logging and reporting, documenting all traffic and security violations</li> </ul>
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (E PHI)	<ul style="list-style-type: none"> <li>Both STM and UTM perform anti-malware scanning to ensure that file integrity has not been compromised by malware</li> <li>UTM includes IPsec and SSL VPNs with built-in mechanisms to ensure data integrity</li> </ul>
Person or Entity Authentication	164.312(d)		<ul style="list-style-type: none"> <li>UTM/STM management is protected via login/password to prevent unauthorized access</li> <li>UTM authenticates users based on user directories to provide secure access to VPNs</li> <li>UTM IPsec and SSL VPNs support two factor authentication for higher levels of control over access, requiring a smart card, token, or key</li> </ul>
Transmission Security	164.312(e)(1)	Integrity Controls	<ul style="list-style-type: none"> <li>Supports standard network protocols such as TCP and UDP in which data integrity is built in</li> </ul>
		Encryption	<ul style="list-style-type: none"> <li>The UTM firewall VPN automatically encrypts electronic transmissions using industry-standard algorithms such as DES, 3DES, AES (128, 192, 256 bit), SHA-1, and MD5</li> </ul>

Table 1: HIPAA Safeguard Requirements Addressed by NETGEAR ProSecure UTM and STM Appliances

## Beyond HIPAA to PCI, Privacy Laws, Web 2.0, and User Productivity

The same security layers that help you achieve key HIPAA mandates can also help with other regulatory requirements and combat a range of threats to your business. For instance, PCI DSS requires companies that handle credit card data to protect that data with firewalls, encryption, anti-virus, strong access controls, and monitoring.<sup>5</sup> Many of these requirements mirror the list in the HIPAA chart above.

Further, at least 48 US states and many countries require disclosure of breaches of personal information, such as addresses, driver license numbers, or Social Security Numbers. A breach that releases this information may also release the EPHI protected by HIPAA. Any breach is expensive and damaging to your reputation. In addition, unrestricted web use can also expose your business to sexual harassment or discrimination lawsuits due to inappropriate content in the workplace.

When it comes to compliance, strong security makes good business sense. Meeting one set of regulations can mean satisfying multiple regulators and audits more efficiently and cost-effectively.

The NETGEAR ProSecure UTM or STM appliance you use for HIPAA and other regulatory compliance can also protect your organization from the fast-changing risks inherent in email, the web, and other networked applications. For example, most companies are concerned about spam and email attachments that can have malicious content. At a minimum, spam clogs your network and takes up space on your server. Worse, infected email attachments can turn an employee's computer into a zombie controlled by a criminal—both to seize your confidential and customer information and to use for illegal activities.

These same types of malicious activities are now common on the web. Criminals corrupt interactive, loosely secured Web 2.0 sites with data-stealing malware, keyloggers, Trojans, and other dangerous code. Visiting a compromised site or downloading an altered PDF or Flash file can bring the same risks you fear from email.

ProSecure UTM and STM appliances can block risky sites and drop malicious content before it reaches your network, applying content security tools such as URL filtering, anti-spam, and anti-malware. They also offer application-layer controls to restrict access to common risky and unproductive applications, such as peer-to-peer file sharing or instant messaging.

Beyond the risks in web, email, and networked applications, hackers and freeloaders will try to gain access to your network, entering it to see what information they can find, or to use your bandwidth to conduct their business. Restricting and controlling who uses your network is critical to protecting your assets and keeping your network available for legitimate business. The versatile ProSecure UTM appliance adds intrusion prevention, firewall, VPN, and application control to its robust content controls to protect your business from these especially subtle and damaging risks.

<sup>5</sup> Refer to our companion paper "How NETGEAR ProSecure UTM Helps Small Businesses Meet PCI Requirements" for details.

## Get Started

By meeting HIPAA administrative and technical safeguards, helping you with other regulations, and protecting your business against lost productivity and modern Internet threats, the NETGEAR ProSecure UTM and STM stretch your security and compliance investment for maximum value. Learn more at [www.prosecure.netgear.com](http://www.prosecure.netgear.com).

## About NETGEAR ProSecure Gateway Security Appliance Solutions

The ProSecure STM and UTM Gateway Security Appliances feature a proven firewall, SSL and IPsec VPN support, IPS, and enterprise-class content security filters to prevent unauthorized access to system components inside the company network.

Patent pending Stream Scanning technology is designed to scan data streams as they enter the network. With Stream Scanning, the NETGEAR STM and UTM process large amounts of data in real time, using a single scan to identify spam, malware, security breaches, or unnecessary applications. This ensures that users on the network receive their email and web content clean of risky content and without delay.

The ProSecure STM and UTM Gateway Security Appliances offer straightforward installation and maintenance. The STM is a transparent bridge that seamlessly integrates into existing network architectures. The UTM is an all-in-one network security solution that replaces any existing firewall or router. Each solution comes equipped with all the security software needed for your business with no per user licenses required.

NETGEAR, the NETGEAR logo, Connect with Innovation, ProSafe, ProSecure and ReadyNAS are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Information is subject to change without notice.  
© 2010 NETGEAR, Inc. All rights reserved.