



Network Security Solutions for Healthcare – HIPAA and Beyond

This document provides an overview of HIPAA regulations, with particular emphasis on the final Security Rule. It presents SonicWALL's broad range of cost-effective Internet security solutions, outlining how they can help healthcare organizations meet HIPAA requirements.

Updated March 2003

CONTENTS

Introduction	2
HIPAA Legislation.....	2
HIPAA Standards.....	4
HIPAA Security Rule	5
SonicWALL Solutions for HIPAA Compliance.....	9
Conclusion.....	15

FORTRESS Network Security

3600 Chamberlain Ln., Ste. 418
Louisville, KY 40241

T: 866.948.7377
F: 502.491.1570

www.fortressnetworksecurity.com



Introduction

The Internet is changing the way healthcare organizations do business – offering healthcare professionals the opportunity to share vast amounts of information. This, in turn, increases efficiency and reduces costly paper-based processes. Healthcare networks are now being used to transmit vital prescription, billing and insurance information, making it readily accessible to those who need it, regardless of their location. Patients can log onto special hospital Web portals to access their medical records, check lab results, or schedule inquiries online. Physicians can work remotely from their home office, downloading and reviewing patient files.

As more and more medical information is converted into electronic format and networks connect to the Internet, systems become increasingly vulnerable to unauthorized users. Healthcare providers now face the challenge of securing information and maintaining strict levels of patient confidentiality while still allowing easy access to authorized users. Cyber terrorism threats compound this issue, creating an even greater sense of urgency as healthcare entities attempt to secure patient information from breach by foreign sources that could potentially use it to create local, regional, or national healthcare terror.

Recognizing the huge importance of protecting patients' privacy, the US Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996. HIPAA regulations require healthcare organizations to take added precautions to ensure the security of their networks and the privacy of their data. As a result, many healthcare IT executives are now scrambling to identify and eliminate security holes that expose their networks to external security threats. According to a recent survey conducted by Phoenix Health Systems in conjunction with HIMSS (Winter 2003), many of them are seriously behind schedule. Only 9% of Providers and 5% of Payers have actually completed Privacy remediation, only 37% of respondents expect to be ready for the Transaction and Code Sets deadline in April of this year and 60% of respondents are still doing gap and risk analyses for the final Security Rule.

Healthcare organizations also are facing considerable challenges in trying to comply with HIPAA regulations. Many are dealing with large, fragmented information networks, IT staffing shortages and severe cost restraints. They require simple, affordable solutions that enable confidential information to flow easily and securely between doctors, hospitals, insurance carriers and patients. The purpose of this paper is to provide an overview of HIPAA regulations, with particular emphasis on the final Security Rule. This paper will present SonicWALL's broad range of cost-effective Internet security solutions, outlining how these solutions can help healthcare organizations meet HIPAA regulations while securing their networks for the future.

HIPAA Legislation

Overview

On April 12, 2001 the Health Insurance Portability and Accountability Act (HIPAA) became law. HIPAA regulations are designed to improve efficiency and effectiveness through the use of electronic healthcare transactions. In doing so, data collection and paperwork burdens can be dramatically reduced, confidential patient information can be properly protected and costly healthcare errors can be avoided.

HIPAA requires that the healthcare industry protect the privacy of patient records and promotes a uniform security standard for the electronic transmission of patient-identifiable information. Existing systems used to store and access electronic data will have to be reevaluated. If they lack the capacity for adequate access control or auditing they will need to be enhanced or replaced.

Organizations are also required to appoint a HIPAA Manager to plan, implement and document an organization's compliance with HIPAA regulations. This individual must record every step that helps prove the organization has implemented technologies and /or procedures to fulfill the requirements.

Who is Affected?

HIPAA applies to almost all segments of the healthcare industry involved in the electronic transmission of health information containing content that could compromise patient confidentiality.

The HIPAA mandate covers a broad range of organizations:

- ▶ All health plans, including government and military health programs, HMO's, indemnity insurers and employer benefit plans
- ▶ Healthcare providers
- ▶ Healthcare services and suppliers
- ▶ Healthcare clearinghouses – companies who process business transactions
- ▶ All healthcare business associates such as accountants and practice management consultants

In other words, HIPAA affects hospitals, doctors and insurance companies as well as pharmacies, optometrists, nursing homes, dentists, medical equipment providers, ambulance companies, assisted living centers, etc. Organizations that maintain paper-based patient files are not required to follow these technical guidelines.

Deadlines and Penalties

Compliance deadlines are rolling based on the finalization dates of each rule - usually 24 months from the date of completion (36 months for small health plans). Compliance dates vary:

- ▶ Standards for Electronic Transactions and Code Sets – October 16, 2002 (October 16, 2003 for those that filed extensions)
- ▶ Standards for Privacy of Individually Identifiable Health Information – April 14, 2003
- ▶ Security Rule – April 21, 2005
- ▶ Electronic Signatures Standard – Under Review
- ▶ National Standard Healthcare Provider Identifier – Under Review
- ▶ National Standard Healthcare Employer Identifier – Drafted, Under Review

The Federal Government has established monetary and criminal penalties for healthcare organizations that fail to comply with the requirements:

- ▶ Failure to meet the compliance deadlines results in non-payment of Medicare claims
- ▶ Violations of any HIPAA stipulations may result in fines of up to \$100 per incident with a maximum of \$25,000 per year
- ▶ Wrongful disclosure of protected healthcare information can result in a fine of \$50,000
- ▶ Offense under false pretenses carries a penalty of \$100,000 and/or imprisonment
- ▶ Offense with intent to sell information results in a \$150,000 fine and/or imprisonment

The Department of Health and Human Services (DHSS) is currently developing a proposed rule on enforcement procedures. The Centers for Medicare and Medicaid Services (CMS) will be tasked with ensuring compliance. It is expected that they will aim to provide education and technical assistance to those who need to achieve compliance rather than imposing immediate penalties. Should such efforts fail, then civil monetary penalties will be imposed.

Aside from complying with HIPAA, healthcare organizations on the whole are facing increasing pressure to protect confidential patient information. Many legal experts believe that regardless of the HIPAA Security mandates, healthcare organizations could be sued in state courts if patient information is compromised or released. Clearly, this represents a significant and immediate risk.

Healthcare organizations also store a considerable amount of confidential patient and corporate data that, if released, could have a devastating impact on public perception. For example, by law, hospitals are required to record every medical error that occurs at the facility. Yet, if this information were obtained and released to the public, the damage incurred on the reputation of the hospital would be extremely difficult to resolve.

Finally, once inside the network, there is the potential for hackers to actually impact the quality of patient care. Databases housing patient records and lab results could potentially be altered resulting in compromised patient care. Terrorists could break into these networks creating havoc on a local, regional or national level. By complying with HIPAA and effectively rooting out all possible Internet threats, healthcare entities can eliminate rogue accounts, close exposed backdoors to their network and provide a much clearer picture of system vulnerabilities.

HIPAA Standards

Electronic Transactions and Code Sets Rule

Today many healthcare providers and plans use Electronic Data Interchange (EDI) for the digital exchange of standard business documents and data. In fact, the Department of Health and Human Services (DHHS) estimates that 400 different formats are currently being used for healthcare claims processing. This lack of standardization not only increases costs for healthcare providers and health plans, but it also inhibits potential efficiencies and makes it difficult for vendors to develop appropriate software.

The Electronic Transactions and Code Sets rule provides a framework for the establishment of a comprehensive set of standards for the electronic transmission of healthcare information. This rule outlines requirements for all healthcare related transactions, including claims, insurance applications and payment processing. The use of industry-wide standards is expected to result in operational efficiencies and long-term savings while eliminating the need for software applications to be continuously adapted to meet proprietary requirements. Compliance with this rule was required by October 16, 2002 or October 16, 2003 for those that filed an extension. Covered entities are required to be ready for transaction testing by April 16, 2003.

Privacy Rule

Traditionally, individual healthcare organizations wishing to ensure the privacy of patient data had to rely on inconsistent state laws and regulations that were both incomplete and contradictory. Personal health information was often distributed without notice or consent and for reasons that had nothing to do with a patient's medical treatment or healthcare reimbursement. For example, patient information held by a health plan was available to a lender who could use it to deny a home mortgage or an employer who would use it in personnel decisions. On April 14, 2001, the

HIPAA Privacy Rule came into effect. Under this rule, healthcare organizations have to guarantee their customers that private information collected, maintained, used or transmitted will remain entirely confidential in order to administer plans and provider services.

The Privacy Rule reflects five basic principles:

- ▶ **Consumer Control** – Consumers are provided with new rights to control the release of their medical information
- ▶ **Boundaries** – With few exceptions, an individual's healthcare information can be used for health purposes only, including treatment and payment
- ▶ **Accountability** – Violation of a patient's right to privacy will result in federal penalties
- ▶ **Public Responsibility** – A balance must be achieved between privacy protections and the public responsibility in order to support such national priorities as protecting public health, conducting medical research, improving the quality of care and fighting healthcare fraud and abuse
- ▶ **Security** – Organizations entrusted with health information must protect it from deliberate or inadvertent misuse or disclosure

Struggling with the issue of how the healthcare system can provide maximum protections for patient privacy without compromising either the availability or quality of medical care, the DHSS proposed significant modifications to the Privacy Rule on August 14, 2002. Most health plans and healthcare providers that are covered by the new rule must comply with the new requirements by April 14, 2003.

HIPAA Security Rule

Compliance Deadlines

On February 20, 2003 the security standards were published as a final rule in the Federal Register, with an effective date of April 21, 2003. Most healthcare organizations including providers, claims clearinghouses and payers, will have two years to fully comply with the Security Rule (until April 21, 2005). However, very small payers with annual receipts below \$5 million will have an additional year to comply (April 21, 2006).

While the above deadlines may encourage some healthcare entities to delay implementation of the Security Rule, it should be noted that the security provisions proposed in this rule constitute sound business practice for any healthcare organization. In addition, with a compliance date of April 14, 2003, the final Privacy Rule requires that covered healthcare organizations provide for the security of protected healthcare information. CFR 45§ 164.530(c) states that “a covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.” In fact, many of the same measures used to protect the integrity of data also serve to protect that data from being shared with those who do not have a legitimate need or permission to access it.

The bottom line is that healthcare organizations must begin taking action on security protections – delaying the implementation of a security policy could pose significant risk in terms of potential non-compliance with the Privacy Rule, and continued information security risk to the organization.

Features of the Final Security Rule

The final Security Rule is designed to be comprehensive and coordinated, addressing all aspects of security. It is also far more simplified than the original draft rule. The Department of Health and Human Services (HSS) has recognized that entities affected by this regulation are so varied in terms of installed technology, size, resources and relative risk that it would be impossible to dictate a specific solution or set of solutions that would be appropriate for everybody. Therefore the Security Rule is designed to be scalable so that it can be implemented by covered entities of all types and sizes, from the smallest provider to the largest clearinghouse. Each healthcare organization must assess its own security needs and risks and implement appropriate security measures accordingly.

This scalability has been achieved by reducing the number of procedures or technologies that must be implemented by healthcare organizations in order to ensure compliance with the standards. According to the matrix in the final rule, only 20 “implementation specifications” are now required, with a further 22 identified as being “addressable”. Addressable implementation specifications require the organization in question to decide whether or not they are appropriate for use in their particular compliance efforts. In making this decision it is expected that the healthcare organization will take into account a variety of different factors, including risk analysis, risk migration strategy, security measures already in place and the cost of implementation. Based on the results of this decision process, the entity may decide to (1) implement the specification (2) implement an alternative security measure to accomplish the purpose of the standard or (3) not implement anything on the basis that the specification is unreasonable or inappropriate and that the standard can still be met by other means.

The final security requirements are also designed to be technically flexible. Given the speed with which technology evolves, healthcare organizations need to be allowed to make use of future technology standards. As a result, the final rule offers more high-level guidance, providing what is essentially a model for information security, with less specific guidance on how to implement that model. However, the adopted security solutions should work as a unified system and not as a series of different products that do not communicate with each other.

General Rule Provisions

HIPAA’s Security Rule defines security standards as a series of requirements and implementations that healthcare organizations must adopt to ensure the security of individuals’ electronic health information. It requires healthcare organizations to:

- ▶ Protect the integrity, confidentiality and availability of all electronic patient information collected, maintained, used or transmitted
- ▶ Protect against any anticipated threats or hazards to the security or integrity of this information
- ▶ Protect against any anticipated uses or disclosures of this information that are not permitted/required by the Privacy Rule
- ▶ Ensure compliance by the entire workforce, whether they are based on site or at home

The final Security Rule identifies three categories of requirements that a covered entity must address in order to ensure the security and integrity of electronic patient information.

Administrative Safeguards

Administrative Safeguards focus on the security management process, including the procedures and policies that are designed to prevent, detect, contain and correct security violations. Some key points include:

- ▶ **Internal Audit** – A covered entity must identify the risks to vulnerabilities of the information in its care before it can take effective steps to eliminate or minimize those risks. Therefore healthcare organizations are asked to conduct an in-house review of the records of system activity that they maintain (e.g. logins, file access and security incidents).
- ▶ **Assigned Security Responsibility** – A single individual must be assigned responsibility for planning, implementing and documenting an organizations compliance with the Security Rule.
- ▶ **Information Access Control** – Information access management controls should be implemented, including addressable standards for access authorization, establishment and modification.
- ▶ **Training** – Training should include user education concerning virus protection, the importance of monitoring login success/failure and user password management.
- ▶ **Security Incident Procedure** – A formal, documented report and response procedure must be created so that security violations can be reported and handled promptly.
- ▶ **Business Associate Contracts and Other Arrangements** – A written agreement must be established between the business partner and the healthcare organization stating that the business partner will appropriately safeguard electronic protected health data in accordance with the standards. If the business associate violates this agreement their contract may be terminated.

Physical Safeguards

Physical Safeguards relate to the protection of physical computer systems, buildings and equipment from fire, environmental hazards and physical intrusion. This section also covers the use of locks, keys and administrative measures that control access to computer systems and facilities. Some key points include:

- ▶ **Facility Access Controls** – Facility access controls provide for access control and validation procedures (staff and visitors) and for the collection of appropriate maintenance records for the physical components of a facility related to security.
- ▶ **Device and Media Controls** – Formal documented policies and procedures must be developed to govern the receipt and removal of hardware and/or software into or out of a facility.

Technical Safeguards

Technical Safeguards contain provisions extracted from two sections of the proposed Security Rule – Technical Security Services and Technical Security Mechanisms. This section contains the following provisions:

- ▶ **Access Control** - The final Security Rule requires both user identification and provision for emergency access procedures. This rule also states that the use of any appropriate access control mechanism is allowed – i.e. an entity does not necessarily have to use role, context or user-based access control. Under the new rule, both automatic logoff and encryption are listed as addressable implementation specifications. While encryption in this context relates to data at rest, it is up to each healthcare organization to conduct a risk analysis to determine whether or not they need to provide encryption for the purpose of access control.
- ▶ **Audit Controls** – Under the final Security Rule, healthcare organizations are still required to put audit control mechanisms in place to record and examine system activity.

By using risk assessment and risk analysis, an entity can determine exactly how intensive their audit control functions need to be.

- ▶ **Integrity** – Integrity replaces “data authentication” in the original Security Rule. However, the concept is still the same. A healthcare organization needs to be able to corroborate that data in its possession has not been altered or destroyed in an unauthorized manner.
- ▶ **Person or Entity Authentication** – A healthcare organization is required to implement procedures to verify that a person or entity seeking access to protected electronic data is who they claim to be.
- ▶ **Transmission Security** – The Transmission Security rule replaces the original Communications and Network Controls rule and has been greatly simplified to reflect one key requirement. When electronic protected data is transmitted from one point to the next it must be protected in a manner appropriate for the level of risk involved. To this effect, the use of integrity controls and encryption are encouraged. Integrity controls can be used to ensure that the data has not been improperly modified without detection while the use of encryption is encouraged when transmitting electronic patient information over the Internet.

Overview of Technology-based Security Requirements

HIPAA’s basic security requirements are clear – healthcare entities need to detect and prevent security breaches. In achieving this, a number of key areas need to be considered:

- ▶ **Access Control** - The security solution adopted must provide the technological capability to enforce the policies and procedures that define who in the organization can have access to what information, for what purposes and the conditions for granting as well as terminating access. A procedure for emergency access is also required.
- ▶ **Authentication** – Each organization must provide validation that the data in its possession has not been altered or destroyed in an unauthorized manner. In addition, each organization must provide entity authentication to ensure the correct identification of an individual accessing secure data.
- ▶ **Audit Controls** – Healthcare organizations need to provide in-house reviews or audits of the records of system activity. Such reviews could include logins, file access and security incidents. This audit capability will enable the organization to identify suspect data access activities, assess its security program and respond to potential weaknesses. The Security Rule does not establish the type or frequency of audits – such determinations will be made by the organization based on its systems and needs.
- ▶ **Transmission Security** - Each organization that uses networks to communicate is required to protect information that is transmitted electronically over these networks. This information must not be intercepted by parties other than the intended recipient and must be protected from intruders trying to gain access from external communication points. HIPAA recommends some form of encryption, particularly for an inherently insecure medium such as the Internet.

SonicWALL Solutions for HIPAA Compliance

Compliance with HIPAA will force healthcare organizations to undertake a number of projects, including the installation, management and monitoring of information security technologies. Since no one technology will suffice to achieve complete security, healthcare organizations will need a layered approach to protect their data and their networks.

SonicWALL provides a comprehensive range of security solutions designed to assist healthcare organizations of all sizes to comply with HIPAA legislation. SonicWALL solutions address a broad range of issues such as network protection, user authentication, encryption and network monitoring and management.

Firewalls for Network Protection

Using a method called IP-spoofing, a hacker masquerading as a trusted IP address could potentially gain access to a hospital network and alter medical data without being detected. This unauthorized access to the hospital's network could, in turn, jeopardize other business associates networks, such as that of the clearinghouse or provider who are now vulnerable to "back door" attacks. More hacker attacks could occur as healthcare data is transmitted from one site to another over the Internet. Hackers armed with packet sniffer programs could intercept and alter this data without the source or destination users ever being aware of it.

A firewall can act as a healthcare organization's first line of defense against these kinds of Internet security attacks. Firewalls effectively implement an access control policy as outlined in the Technical Safeguards category of the Security Rule. Using predetermined security policies, a firewall allows only authorized traffic to pass through the network perimeter. In effect, it acts as a gateway, filtering traffic passing between the protected "inside" network and the less trustworthy "outside" network. By protecting the perimeter of the environment, firewalls are able to guard against common attacks such as denial of service, security breaches or configuration changes.

Like a "phone tap" or tracing tool, firewalls can also generate summaries about the kinds and amounts of traffic passing through and how many attempts are made to break into the network. This logging and auditing function enables the network administrator to comply with the audit controls requirement as outlined in the Technical Safeguards category.

SonicWALL offers a complete range of high-performance enterprise-class firewalls that deliver stringent security without impacting a network's performance.

SonicWALL Firewalls deliver the following benefits:

- ▶ **Scalable** – Solutions scale from telecommuters to small-to-medium sized healthcare organizations to large HMOs
- ▶ **Industry Standard** – All SonicWALL firewalls are ICSA-certified for compliance with industry standards
- ▶ **Robust** – Powerful architecture includes a security ASIC for superior firewall and 3DES VPN performance
- ▶ **Flexible** – SonicWALL firewalls can be upgraded to include additional nodes and VPN support
- ▶ **Easy of Installation** – Web-based management and installation wizards simplify installation
- ▶ **Ease of Use** – SonicWALL's "1-click update" automatically pushes out new firewall features and software updates to keep users abreast of the latest security threats

VPN for Secure Remote access

When engaging in risk analysis, healthcare organizations must also consider how to provide and control access for individual employees working outside of the organization. This scenario could apply to employees working from home or on the road as well as business associates and contractors.

Often hackers unable to gain access to a network through an Internet Gateway will bypass the Gateway and exploit a remote access systems (RAS) with weak access controls. Remote attack vulnerabilities (such as dial-in servers) are a frequent point of access for hackers.

By establishing a Virtual Private Network (VPN), healthcare organizations can create private, secure communications across a public network (e.g. Internet) thereby safely extending their networks to remote clinics, or physicians who telecommute. VPN solutions also enable healthcare entities to realize dramatic cost savings since they are using the public Internet as opposed to expensive leased lines or frame relay.

SonicWALL offers a range of VPN-enabled firewalls to deliver fast, secure access to network resources as well as a VPN software client solution for professionals working remotely.

SonicWALL VPN solutions deliver the following benefits:

- ▶ **User-level Authentication** - Requires remote users to authenticate themselves to a server and the server to authenticate itself to the remote user – this prevents a third party from trying to impersonate the remote user or the server
- ▶ **IPSec Compliance** – Enables SonicWALL's hardware and software-based VPN solutions to work with any manufacturer's IPSec-compliant VPN gateway, including products from Cisco and Check Point
- ▶ **Manageable** –SonicWALL's Global Management System (GMS) software facilitates easy management of multiple VPN connections whether they are being used for remote access or site-to-site connectivity
- ▶ **Network Address Translation (NAT) Support** – SonicWALL's VPN Client increases secure network access flexibility by allowing IPSec VPN traffic to pass through any IP network using NAT

Encryption for Secure Remote Access

The Security Rule recommends the use of encryption when transmitting data over an inherently insecure medium such as the Internet. Encryption technology ensures that any messages traveling across the VPN cannot be easily intercepted or read by anyone other than the authorized recipient. This is achieved by using advanced mathematical algorithms to "scramble" messages and their attachments.

While the encryption process must be strong enough to ensure that private information sent over the Internet remains private, it must also be implemented in a way that does not significantly affect network performance. The procedure for distributing keys is also critical – it must be scalable in order to make using a VPN cost effective for smaller healthcare entities.

SonicWALL firewalls offer 3DES encryption for secure data transmissions over a VPN tunnel. By offloading processing overhead associated with encryption, the SonicWALL security ASIC guarantees the best possible VPN performance from broadband connections.

[Complete Anti-Virus for Network Protection](#)

Virus checking is vital to ensure the integrity of electronically transmitted patient data over an open network such as the Internet. Virus attacks are one of the greatest security threats today and statistics show that outbreaks continue to increase. According to a recent survey conducted by the FBI and the Computer Security Institute (Spring 2002) 90% of respondents had detected computer breaches within the previous 12 months while 85% reported encountering computer viruses.

These destructive programs attach themselves to applications and files, quickly damaging an entire network or opening up network resources to hackers. Developed in partnership with McAfee, SonicWALL offers a complete anti-virus solution designed to protect systems from viruses that could affect the availability and integrity of data. This solution consists of an award-winning policy enforced anti-virus client (patent pending), NetShield and GroupShield server anti-virus applications and rapid email attachment blocking.

SonicWALL anti-virus solutions deliver the following benefits:

- ▶ **Faster Time to Protection** – “Rapid email attachment blocking” protects in hours rather than days by blocking harmful virus/ worm-specific attachments even before the virus signatures are made available
- ▶ **Enforced Protection** – Automatic anti-virus policy enforcement requires users to receive the latest anti-virus updates before logging on to the Internet. This also guarantees that the client is always present and active
- ▶ **Lowest total cost of ownership** – It is estimated that maintenance accounts for approximately 80% of the total cost of any anti-virus solution. SonicWALL’s anti-virus solution features easy to manage client auto-installation, virus definition updates and enforcement of virus protection through any SonicWALL firewall

[Global Management System Software for Manageability and Reporting](#)

The Security Rule requires healthcare organizations to adopt audit control mechanisms to record and examine system activity. Audit controls can help healthcare organizations to uncover suspect data activity and determine the effectiveness of their security policies and procedures. Audit controls can also assist in establishing accountability and identifying potential threats stemming from unauthorized or inappropriate use of the information

In order to manage and audit a network, an events log is needed. The log should automatically record important events such as the addition or deletion of a user as well as session start and end data. One of the most important events to track is unsuccessful user logins – these can be studied to help determine if someone is attempting to attack the network.

SonicWALL’s Global Management System software (GMS) is a Web-based graphical reporting tool designed to help administrators understand and manage their networks by turning comprehensive log data from SonicWALL firewalls into meaningful reports without using complex and expensive commercial reporting packages.

GMS also enables healthcare organizations to implement a single security policy throughout their network, saving time, reducing errors and simplifying their auditing process. With SonicWALL’s Global Management System software, network administrators can centrally manage all firewalls, value-added services and VPN gateways and connections from one location.

SonicWALL's Global Management System (GMS) delivers the following benefits:

- ▶ **Comprehensive** – Reports can cover firewall attacks, bandwidth usage, Web site visits, user activity and more
- ▶ **Ease-of-use** – GMS provides graphic, high-level summaries of log data that are easy to understand
- ▶ **Scheduled Reports** – GMS allows you to schedule a wide range of reports to provide insight into usage trends and security events
- ▶ **Flexibility** – GMS can be managed from any secure Web browser, reducing the need to focus administration resources in one location and providing a flexible way to segment and distribute management responsibility amongst several individuals
- ▶ **Scalability** – GMS can easily support a growing network and ensure network security, reliability and efficient bandwidth distribution

Secure Socket Layer Technology for Secure Web Transactions

Web-based services and applications promise to be the foundation for HIPAA compliance. However, Web sites delivering confidential medical information require security to protect the data as it passes over the Internet. Most secure Web servers use the industry-standard Secure Socket Layer (SSL) protocol to identify the server to the user and secure the transaction between them using encryption. This protects against eavesdropping, tampering and forgery. However, processing these SSL-based transactions can put a heavy load on Web servers, resulting in lost productivity, frustrated users and lost revenues.

SonicWALL's SSL Offloaders deliver cost-effective, high performance solutions for boosting the performance of secure servers by completely offloading the burden of all SSL processing from Web servers. These are secure, robust solutions with RC4-128-MD5 at 100+ Mbps providing the ability to manage 4,400 RSA operations per second and 30,000 concurrent connections. They can be easily installed into any production network and integrated seamlessly with a secure content switch networking hardware.

Standards (R) = Required Implementation Specification (A) = Addressable Implementation Specification	SonicWALL Solutions	SonicWALL Products
Access Control §164.312(a)(1) <ul style="list-style-type: none"> • Emergency Access Procedure (R) • Encryption and Decryption (A) • Automatic Logoff (A) • Unique User Identification (R) 	<p>SonicWALL firewalls control incoming and outgoing traffic between the Internet and protected networks.</p> <p>SonicWALL firewalls feature “use inactivity time out” to log off users who have been inactive for a predetermined length of time.</p>	<p>SonicWALL Firewalls</p> <ul style="list-style-type: none"> • TELE3, TELE3 TZX, TELE3 SP • SOHO3 • PRO 100 • PRO 230 and PRO 330 • GX250 and GX650
	<p>SonicWALL VPN enables you to determine who gets access to the network using User Level Authentication. Users can easily be added or removed from the list.</p>	<ul style="list-style-type: none"> • SonicWALL firewall/VPN appliances • SonicWALL Global VPN client
Audit Controls §164.312(b) (R)	<p>Both SonicWALL firewalls and GMS offer logging and reporting features enabling you to see who has accessed what information, what their IP address are, hacker attacks that have been prevented by the firewall. etc.</p>	<p>SonicWALL Firewalls</p> <ul style="list-style-type: none"> • TELE3, TELE3 TZX, TELE3 SP • SOHO3 • PRO 100 • PRO 200 and PRO 300 • GX250 and GX650
	<p>SonicWALL Global Management System enables you to generate a report on network activity so that you can see changes made to firewall policies or VPN tunnels.</p> <p>SonicWALL GMS reporting software enables you to generate a report on DOS attacks.</p>	<p>Global Management System (GMS) Software</p>
Integrity §164.312 (c)(1) <ul style="list-style-type: none"> • Mechanism to Authenticate Electronic Protected Health Information (A) 	<p>SonicWALL firewalls utilize data authentication algorithms to ensure that encrypted data sent over the firewall is not altered or tampered with.</p>	<p>SonicWALL Firewalls support</p> <ul style="list-style-type: none"> • SHA1 • MD5
	<p>SonicWALL Complete Anti-Virus protects networks from harmful viruses and worms.</p>	<p>SonicWALL Complete Anti-Virus</p>

Standards (R) = Required Implementation Specification (A) = Addressable Implementation Specification	SonicWALL Solutions	SonicWALL Products
Person or Entity Authentication §164.312(d) (R)	<p>SonicWALL firewalls feature an internal user database that can authenticate users through the usernames and passwords.</p> <p>To authenticate larger numbers of users, SonicWALL firewalls feature RADIUS support whereby the RADIUS server verifies the identity of the user before allowing them through a VPN tunnel.</p>	<p>SonicWALL firewalls support</p> <ul style="list-style-type: none"> • SHA 1 • MD5 • RADIUS
Transmission Security §164.312(e)(1) <ul style="list-style-type: none"> • Integrity Controls (A) • Encryption (A) 	<p>SonicWALL SSL Offloaders protect confidential patient information as it passes over the Internet.</p>	<p>Secure Socket Layer (SSL) Offloaders</p>
	<p>SonicWALL VPN enables you to determine who gets access to the network by using User Level Authentication. Users can easily be added or removed from the list.</p>	<p>SonicWALL VPN Client</p>
	<p>SonicWALL's VPN solution includes 3DES encryption at rates up to 285Mbps. SonicWALL's SSL solution includes RC4-128-MD5 @ 100+ Mbps.</p>	<p>Encryption</p>

Conclusion

HIPAA will undoubtedly cause major organizational and financial disruptions for many healthcare providers. For some, the Security Rule may be particularly daunting because it involves sophisticated information technology (IT) concepts and components that might not be available in their existing IT environment. Not surprisingly, many concerns will also exist about expensive, complex and time-consuming system upgrades. On the whole, compliance will require organizations to develop a detailed understanding of their IT systems in order to address their vulnerabilities.

However, implementation of a sound security strategy and the practice of ongoing security risk management is the best approach to meet the changing demands of today's healthcare industry. For many reasons, adopting the requirements of HIPAA's Security Rule makes good business sense. An organization lacking adequate protection risks inadvertent disclosure of patient data, with resulting loss of public trust and potential legal action. Hacking and other security violations may be widely publicized, and can seriously damage an institution's community standing. In addition, appropriate security protections are crucial for encouraging the growth and use of electronic data interchange. Given the threats facing organizations today the potential cost of not reasonably addressing security risks could substantially exceed the cost of compliance.

SonicWALL security solutions enable healthcare organizations of all sizes to realize the many benefits of HIPAA compliance. SonicWALL's family of products and services help protect vital medical information on networks, while allowing confidential information to flow easily and securely between doctors, hospitals, insurance carriers and patients. With cost-effective, flexible and easy-to-administer solutions from SonicWALL, healthcare organizations can both meet and exceed HIPAA requirements.

