

Healthcare Network Security Solutions HIPAA and Beyond

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

Contents

| | |
|--|----|
| HIPAA Legislation | 2 |
| HIPAA Standards | 3 |
| HIPAA Security Rule | 4 |
| SonicWALL Solutions for HIPAA Compliance | 7 |
| Conclusion | 10 |

Abstract:

The Internet is changing the way healthcare organizations do business, enabling healthcare professionals to share vast amounts of information, increase efficiency and reduce costly and error-prone paper-based processes. Healthcare networks transmit vital patient care, billing and related administrative 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 offices, downloading and reviewing patient files.

As more medical information is converted into electronic format and healthcare networks are connected to the Internet, systems become increasingly vulnerable. Healthcare providers now face the challenge of securing information and maintaining strict levels of patient confidentiality while still allowing easy access to authorized users.

Recognizing the 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, most healthcare organizations are now scrambling to identify and eliminate vulnerabilities that expose their networks and sensitive patient information.

In the findings from their fall 2003 survey, the Phoenix Healthcare Systems and the Healthcare Information and Management Systems Society (HIMSS) reported compliance is progressing, but it is still not where it needs to be.

HIPAA Privacy

- Across all industry segments, compliance remains between 73% and 88%.
However, 24% of Providers are non-compliant, six months after the deadline.
- Half of all respondents reported one or more privacy breaches over the past six months

Security

- Half of Providers and Payers report they will not be fully compliant until the April 2005 deadline.
- Nearly 25% of Providers reported one or more data security breaches in the three months prior to October 2003.
- Nearly 30% felt that their organizations were significantly or severely affected by the international computer worm attacks of August 2003.

Healthcare organizations face considerable challenges complying with HIPAA regulations. Many deal with large, fragmented information networks, IT staffing shortages and severe cost constraints. Organizations 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 and present SonicWALL's broad range of cost-effective Internet security solutions—outlining how these solutions 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 a law. HIPAA regulations are designed to improve efficiency and effectiveness through the use of electronic healthcare transactions, dramatically reducing data collection and paperwork burdens, avoiding costly healthcare errors and protecting confidential patient information.

HIPAA requires the healthcare industry to 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 re-evaluated. If they lack the capacity for adequate access control or auditing, they will need to be enhanced or replaced.

Organizations are required to appoint an Information Security Officer (ISO) to plan, implement and document compliance with HIPAA regulations. This individual must record every step that proves the organization has implemented technologies and/or procedures to fulfill the requirements.

Who is Affected?

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

HIPAA mandates cover a broad range of organizations:

- All health plans, including government and military health programs, Managed Care Organizations, indemnity insurers and employer sponsored benefit plans
- Healthcare providers
- Healthcare services and suppliers
- Healthcare clearinghouses—companies who process medical and dental 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, dentists, nursing homes, medical equipment providers, ambulance companies, assisted living centers, etc.

Organizations maintaining paper-based patient files are not required to follow these technical guidelines.

Deadlines and Penalties

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

- **Standards for Electronic Transactions and Code Sets**—4/14/02, ready for testing 04/16/03
- **Standards for Privacy of Individually Identifiable Health Information**—4/14/03
- **Security Rule**—4/21/05
- **Electronic Signatures Standard**—Omitted for Final Rule, but still under review
- **National Standard Healthcare Provider Identifier**—Start applying 5/23/05
- **National Standard Healthcare Employer Identifier**—7/30/04

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

- Failure to meet compliance deadlines results in non-payment of Medicare claims.
- Violations of HIPAA stipulations may result in fines up to \$100 per incident with a maximum of \$25,000 per year.
- Wrongful disclosure of protected healthcare information can result in a \$50,000 fine.
- Offense under false pretenses carries a \$100,000 penalty 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 (DHHS) is currently developing a proposed enforcement procedure rule. The Centers for Medicare and Medicaid Services (CMS) are tasked with ensuring compliance and are expected to provide education and technical assistance to those who need to achieve compliance, rather than imposing immediate penalties. However, should such efforts fail, they will impose civil and criminal penalties.

Beyond HIPAA

Aside from complying with HIPAA, healthcare organizations on the whole are facing increasing pressure to protect patient information. Legal experts believe healthcare organizations could be sued in state courts if patient information is compromised or released, representing a significant and immediate risk.

Healthcare organizations store considerable amounts 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. If this information were obtained and released to the public, the damage to the hospital's reputation would be extremely difficult to remedy.

Finally, once inside the network, there is potential for hackers to access databases housing patient records and lab results, which could be altered, resulting in compromised patient care. By complying with HIPAA and effectively rooting out all possible Internet threats, healthcare entities can eliminate rogue accounts, close exposed back doors 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. DHHS estimates that 400 different formats are currently used for healthcare claims processing. This lack of standardization not only increases costs for healthcare providers and health plans, it inhibits potential efficiencies and makes it difficult for vendors to develop appropriate software.

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

Privacy Rule

Traditionally, individual healthcare organizations wishing to ensure patient data privacy 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. Under HIPAA, 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 provide services.

The Privacy Rule reflects five basic principles:

- 1. Consumer Control**—Consumers have new rights controlling the release of their medical information.
- 2. Boundaries**—With few exceptions, an individual's healthcare information can be used for health purposes only, including treatment and payment.
- 3. Accountability**—Violation of a patient's right to privacy will result in federal penalties.
- 4. Public Responsibility**—Balancing between privacy protections and national priorities such as protecting public health, conducting medical research, improving the quality of care and fighting healthcare fraud and abuse.
- 5. Security**—Organizations must protect health information 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 DHHS proposed significant modifications to the Privacy Rule on August 14, 2002. Most health plans and healthcare providers covered by the new rule were required to 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—effective April 14, 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). 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, the security provisions proposed in this rule constitute sound business practice for any healthcare organization.

The final Privacy Rule (April 14, 2003) requires covered healthcare organizations provide for the security of protected healthcare information. CFR 45§ 164.530(c) states "a covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 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 protection. Delaying the implementation of a security policy could pose significant risk, both 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 DHHS recognized that entities affected by this regulation are so varied in installed technology, size, resources and relative risk, that it would be impossible to dictate a specific solution or set of solutions appropriate for everybody. Therefore, the Security Rule is designed to be scalable, allowing it to 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.

Scalability was achieved by reducing the number of required procedures and technologies. 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 to decide if the specification applies in their particular compliance efforts. In making this decision, the healthcare organization must take into account a variety of different factors, including: risk analysis, risk migration strategy, security measures already in place and the cost of implementation. Adopted security solutions should work as a unified system and not as a series of different products that do not communicate with each other. Based on the results of this decision process, the entity may decide to:

- implement the specification
- implement an alternative security measure to accomplish the purpose of the standard
- or 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 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 a model for information security, with less specifics on how to implement that model.

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 work force, whether they are based on site or at home.

The final Security Rule identifies three categories of requirements 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 procedures and policies designed to detect, prevent, contain and correct security violations. Key points include:

- **Internal Audit**—A covered entity must identify the risks to vulnerabilities of 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 system activity records 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 organization's 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 business partners 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. Key points include:

- **Facility Access Controls**—Procedures for access control and validation (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 the following provisions extracted from two sections of the proposed Security Rule—Technical Security Services and Technical Security Mechanisms.

- **Access Control**—The final Security Rule requires both user identification and provision for emergency access procedures. It also states any appropriate access control mechanism is allowed—e.g. an entity does not 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 data is transmitted from one point to the next it must be protected in a manner appropriate for the level of risk involved. The use of integrity controls and encryption are encouraged. Integrity controls are 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.

SonicWALL Solutions for HIPAA Compliance

Compliance with HIPAA forces 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 need a layered approach to protect their data and networks. SonicWALL provides a range of comprehensive security solutions designed to assist healthcare organization comply with HIPAA legislation by addressing key issues such as network protection, user authentication, encryption, network monitoring and network management.

Firewalls for Network Protection

Using a method called IP-spoofing, a hacker masquerading as a trusted IP address could gain access to a hospital network and alter medical data without being detected. This unauthorized access to the hospital's network could also jeopardize other business associates' networks, such as the clearinghouse or provider, who are now vulnerable to "back door" attacks. Firewalls act as first line of defense against these kinds Internet security attacks.

Firewalls effectively implement an access control policy as outlined in the Technical Safeguards category of the Security Rule. It acts as a gateway, filtering traffic passing between the protected "internal" network and the less trustworthy "external" network.

Like a "phone tap" or tracing tool, firewalls 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 robust security without impacting a network's performance.

SonicWALL Firewalls benefits:

- **Scalable**—Solutions scale from telecommuters to small-to-medium sized healthcare providers to large HMOs
- **Industry Standard**—SonicWALL firewalls are ICSA-certified for compliance with industry standards
- **Robust**—A high-performance hardware platform for superior firewall and VPN performance
- **Flexible**—SonicWALL firewalls are upgradable to support additional security capabilities
- **Easy to Install and Use**—Web-based management and installation wizards simplify installation and use. SonicWALL's auto-update, automatically installs 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, contractors, or business associates working outside of the organization. This could apply to individuals working from home or on the road at remote office locations.

A Virtual Private Network (VPN) enables healthcare organizations to 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 provide dramatic cost savings since they use 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 benefits:

- **User-level Authentication**—Requires remote users to authenticate themselves to a server and the server to authenticate itself to the remote user, preventing 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.

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 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 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 or AES encryption for secure data transmissions over a VPN tunnel. By offloading processing overhead associated with encryption, SonicWALL’s high-performance hardware platforms maximize VPN performance across high-speed Internet 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 2003), 82% reported encountering computer viruses within the last 12 months.

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 that protect systems from viruses affecting 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 E-mail attachment blocking.

SonicWALL Anti-Virus solutions benefits:

- **Faster Time to Protection**—“Rapid email attachment blocking” protects in hours, not days, by blocking harmful virus/worm-specific attachments before the virus signatures are even 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 help organizations uncover suspect data activity and assess the effectiveness of security policies and procedures effectiveness. Audit controls 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 adding or deleting users and 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 (GMS) software is an administration and graphical reporting tool allowing administrators to understand and manage their networks by turning comprehensive log data from SonicWALL firewalls into meaningful reports, without using complex and expensive commercial reporting packages.

SonicWALL's Global Management System (GMS) benefits:

- **Comprehensive**—Reports cover firewall attacks, bandwidth usage, Website visits, user activity and more.
- **Easy to Use**—GMS provides graphic, high-level summaries of log data that are easy to understand.
- **Scheduled Reports**—GMS allows scheduling of a wide range of reports, providing insight into usage trends and security events.
- **Flexibility**—GMS is 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 easily supports a growing network, ensuring network security, reliability and efficient bandwidth distribution.

Mapping SonicWALL to HIPAA

R = Required Implementation Specification **A** = Addressable Implementation Specification

| HIPAA Requirement | SonicWALL Solution |
|--|---|
| Access Controls §164.312(a)(1) <ul style="list-style-type: none"> ■ Unique user identification (R) ■ Automatic logoff (A) ■ Encryption (A) | <ul style="list-style-type: none"> ■ Firewalls block unauthorized access ■ VPN features user-level authentication ■ Inactivity time outs for firewall and VPN sessions ■ VPN features 3DES and AES encryption ■ WLAN security controls wireless access |
| Audit Controls §164.312(b)(R) | <ul style="list-style-type: none"> ■ Firewall collects comprehensive log data, including access attempts and security incidents ■ ViewPoint creates reports from log data ■ SonicWALL GMS reports security and VPN policies changes |
| Integrity §164.312(c)(1) (A) | <ul style="list-style-type: none"> ■ IPSec VPN includes integrity controls to preserve transmitted data integrity ■ Complete Anti-Virus protects network from viruses and worms that compromise data integrity |
| Person or entity authentication §164.312(d) (R) | <ul style="list-style-type: none"> ■ Firewall and VPN authenticates users to internal database or to external database via RADIUS: <ul style="list-style-type: none"> • VPN access • Wireless access • Firewall traversal |
| Transmission security §164.312(e)(1) <ul style="list-style-type: none"> ■ Integrity controls (A) ■ Encryption (A) | <ul style="list-style-type: none"> ■ Site-to-site and remote access IPSec VPN ■ IPSec VPN also assures secure WLAN transmissions ■ VPN features 3DES and AES encryption and IPSec integrity controls |

Conclusion

HIPAA is undoubtedly causing major organizational and technological changes for healthcare entities of all sizes. For some, the Security Rule may be particularly daunting because it involves information technology (IT) concepts and components that are not available in the organization's existing IT environment. Not surprisingly, many concerns also exist about expensive, complex and time-consuming system upgrades. Compliance requires 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 standing in the community. 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 substantially exceeds the cost of compliance.

SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

