

## ▷ SONICWALL SOLUTION BRIEF: SonicWALL SOLUTIONS FOR HIPAA COMPLIANCE

Healthcare organizations face considerable challenges trying to understand and comply with HIPAA regulations. This document provides a brief overview of HIPAA requirements with a focus on the security rule. It describes the HIPAA standards, SonicWALL's healthcare security solutions, and how these solutions can help healthcare organizations meet HIPAA regulations while securing their networks for the future.

### HIPAA Overview

- ▷ Health Insurance Portability and Accountability Act (HIPAA) became law in April 2001.
- ▷ Designed to improve efficiency and effectiveness using electronic data transactions, reducing data collection/paperwork burdens, costly errors and providing proper protection of confidential patient information.
- ▷ Promotes uniform standards for the privacy and security of patient-identifiable information.

#### HIPAA mandates cover a broad range of organizations:

- ▷ Hospitals
- ▷ Doctors offices
- ▷ Insurance companies
- ▷ Nursing homes
- ▷ Medical equipment providers
- ▷ Pharmacies
- ▷ Ambulance companies
- ▷ Dentists and more...
- ▷ Groups with paper-based files are **not covered**

#### Deadlines

- ▷ 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

#### Compliance Progress

- ▷ 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
  - 50% of Providers and Payers 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% of organizations were significantly or severely affected by the 08/03 international computer viruses.

*Taken from the Phoenix Health Systems and the Healthcare Information and Management Systems Society (HIMSS) Fall 2003 Survey*

#### Monetary and criminal penalties

Penalties include non-payment of Medicare claims and fines ranging from \$100—\$150,000 and/or imprisonment, depending on standards breaches, information disclosures and intent.

### HIPAA Standards

#### Electronic Transactions and Code Sets Rule

Comprehensive framework for electronic transmission of information (claims, insurance applications and payment processing, etc)

#### Privacy Rule

Guarantee 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 control the release of their medical information.
- 2. Boundaries**— Information is used for health purposes only—treatment and payment.
- 3. Accountability**— Violations result in federal penalties.
- 4. Public Responsibility**— A balance between privacy and responsibility to public health, medical research, quality of care and fighting fraud and abuse.
- 5. Security**— Protect information from deliberate or inadvertent misuse or disclosure.

## HIPAA Security Rule

### General Rule Provisions

- ▷ Protect the integrity, confidentiality and availability of all electronic patient information collected, maintained, used or transmitted.
- ▷ Protect against any threats or hazards.
- ▷ Protect against any inappropriate disclosures of information.
- ▷ Ensure compliance by the entire workforce—on site or at home.

### Technical Safeguards

Extracted from two sections of the proposed Security Rule – Technical Security Services and Technical Security Mechanisms.

- ▷ **Access Control**—User identification and provisions for emergency access procedures. Automatic log off and encryption are listed as addressable implementation specifications.
- ▷ **Integrity (formerly Data Authentication)**—Corroborate data has not been altered or destroyed.
- ▷ **Person or Entity Authentication**—Verify an entity seeking access is who they claim to be.
- ▷ **Audit Controls**—Audit control mechanisms to record and examine system activity.
- ▷ **Transmission Security**—Electronic data is transmitted in a manner appropriate for the level of risk.

## SonicWALL Healthcare Security Solutions

SonicWALL offers a broad range of easy-to-use, scalable and cost-effective healthcare security solutions—helping to keep a workforce mobile and productive, while meeting HIPAA regulations. These robust solutions are based on industry standards, providing the flexibility to easily integrate into new or existing systems and update as necessary. The SonicWALL TZ, TZW and PRO families secure wired and wireless networks of all sizes, ranging from home offices, telecommuters and remote clinics to complex hospitals systems.

**Firewall/VPN Appliances** protect the perimeter of your network by acting as a gateway against external attacks and allowing only acceptable traffic through. VPN (Virtual Private Network) provides secure, cost-effective connectivity between remote clinics, physician offices, administration and hospitals, allowing only intended recipients to access confidential information.

**Wireless** networking solutions offer unprecedented freedom and flexibility, mobilizing the workforce and bringing productivity applications closer to the point-of-care. SonicWALL solutions use enhanced IPsec security, making them much more secure than the standard Wired Equivalent Privacy (WEP) encryption.

**Anti-Virus (AV) Solutions** keep healthcare organizations running while eliminating costly operational disruptions or shutdowns. AV provides client and server protection, blocking attacks in hours, not days, and ensuring all users have the latest updates before logging on to the Internet.

**Management and Reporting** software simplifies the HIPAA auditing process by turning firewall attacks and user activity log files into meaningful, scheduled reports. With centralized management, a single administrator is able to manage multiple appliances and implement uniform security policies, saving time and reducing errors.

## Mapping SonicWALL to HIPAA

R = Required Implementation Specification

A = Addressable Implementation Specification

HIPAA REQUIREMENT	SonicWALL SOLUTION
ACCESS CONTROLS §164.312(a)(1) UNIQUE USER IDENTIFICATION (R) AUTOMATIC LOGOFF (A) ENCRYPTION (A)	<ul style="list-style-type: none"> <li>• Firewalls block unauthorized access</li> <li>• VPN features user-level authentication</li> <li>• Inactivity time outs for firewall and VPN sessions</li> <li>• VPN features 3DES and AES encryption</li> <li>• WLAN security controls wireless access</li> </ul>
AUDIT CONTROLS §164.312(b) (R)	<ul style="list-style-type: none"> <li>• Firewall collects comprehensive log data, including access attempts and security incidents</li> <li>• ViewPoint creates reports from log data</li> <li>• SonicWALL GMS reports security and VPN policies changes</li> </ul>
INTEGRITY §164.312(c)(1)(A)	<ul style="list-style-type: none"> <li>• IPsec VPN includes integrity controls to preserve transmitted data integrity</li> <li>• Complete Anti-Virus protects network from viruses and worms that compromise data integrity</li> </ul>
PERSON OR ENTITY AUTHENTICATION §164.312(d)(R)	<ul style="list-style-type: none"> <li>• Firewall and VPN authenticates users to internal database or to external database via RADIUS                             <ul style="list-style-type: none"> <li>• VPN access</li> <li>• Wireless access</li> <li>• Firewall traversal</li> </ul> </li> </ul>
TRANSMISSION SECURITY §164.312(e)(1) • INTEGRITY CONTROLS (A) • ENCRYPTION (A)	<ul style="list-style-type: none"> <li>• Site-to-site and remote access IPsec VPN</li> <li>• IPsec VPN also assure secure WLAN transmissions</li> <li>• VPN features 3DES and AES encryption and IPsec integrity controls</li> </ul>