WHITE PAPER

HIPAA:

COMPLIANCE BRIEF

Prepared by: Untangle, Inc.
November 1, 2014

WHAT CONSTITUTES COMPLIANCE?

Perhaps you've been notified through a security audit that your organization is noncompliant with HIPAA as it relates to handling patient data in electronic form (EPHI - Electronic Protected Health Information, in HIPAA parlance). Your firewall and VPN should have you covered, right?

HIPAA regulations such as 164.312(a)(1) Access Control, 164.312(b) Internal Audit, 164.308(e)(1) Transmission Security, and 164.308(a)(5)(ii)(B) Protection From Malicious Software are complex topics. Even the most seasoned IT professionals for whom security is second nature struggle with the mandates of HIPAA.

HIPAA dictates data privacy, but does not specify what measures must be put in place to ensure it. This lack of specificity is one of the most common criticisms of HIPAA.

So what can you do to ensure you pass your HIPAA audit? How can you tell if a given solution will get you to compliance?

INTERPRETING HIPAA

We've extracted key areas of the HIPAA regulation that have to do with (or are affected by) perimeter-based security systems (e.g. a Firewall, VPN and IPS). For each section, exact text from the HIPAA regulation is reproduced, followed by a security/IT interpretation, as well as tips on how to ensure you have (or are correctly selecting) the right product.

This white paper is not intended to be a complete treatment of HIPAA compliance, but rather a succinct guide to determine if your network security infrastructure is helping (or hurting) your chances for a clean HIPAA audit.

There are two primary sections of HIPAA that relate to network security; Administrative Safeguards (Section 164.308) and Security Safeguards (Section 164.312).

ADMINISTRATIVE SAFEGUARDS

164.308(a)(5)(ii)(B) - Protection From Malicious Software
"[Organization must have] procedures for guarding against, detecting and reporting malicious software."

There are many forms of malicious software that can impact data and networking systems. Viruses, worms and trojans are the most prolific threats and are usually introduced via infected email attachments.

Newer threats such as web site cross-scripting, SQL injection attacks and even spyware can affect data and systems. To protect against the predominant delivery mechanisms of malicious software, the security schema must provide:

- Virus and worm protection through gateway and desktop antivirus systems.
- Trojan identification and mitigation, as well as FTP, IM and P2P threat mitigation through Intrusion Prevention (IPS) systems.
- Web content filtering to prevent malware delivered over Port 80 and 443 (web downloads, etc).

What to look for:

Make sure that both desktop and gateway antivirus products are being used at all times.

Ensure that your security gateway is capable of Deep Packet Inspection (DPI) and that it is providing web filtering, application-layer intrusion prevention and gateway antivirus services.

Make sure that the solution's security services provide regular updates of signature files to ensure protection against fast-moving threats like worms. If you are not paying for these security services, that should be a red flag; these services cost vendors money, and if they offer the services for free, you are likely 'getting what you pay for'.

Spyware blocking would be optional for this standard, but it will be needed later on.

Untangle's Next Generation Firewall meets all of the criteria on this list.

RESPONSE AND REPORTING

164.308(a)(6)(ii) - Response and Reporting

"Identify and respond to suspected or known security incidents; mitigate to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."

What to look for:

- Make sure that all of the security services and sub-systems are proactive.
- Make sure that the reporting provided by your firewall is sufficient to both quickly identify incidents as well as respond to them.
- User and group policies are important for identifying usage behaviors and triangulating incidents.

Untangle's Next Generation Firewall meets all of the criteria on this list.

ENCRYPTION AND DECRYPTION

164.312(a)(2)(iv) - Encryption and Decryption [under the Access Control section]

"Implement a mechanism to encrypt and decrypt electronic protected health information."

This standard aims to prevent unauthorized users from accessing PHI (protected health information). Many HIPAA violations stem from weak encryption, lack of encryption, or misuse of encryption.

Any time PHI is sent outside the boundaries of the network, it must be encrypted using a strong encryption methodology such as that defined by IPSec (which uses 3DES or AES encryption). SSL (which uses 3DES encryption) is a fine solution for application-layer encryption, but it does nothing to protect the transport layers (IPSec does this).

While it is usually not critical to store data in an encrypted format, sensitive environments might choose to transport internal data in an encrypted format. SSL is a good option for this.

Note on wireless LAN and WEP: 802.11 WLAN technology has added incredible mobility to the medical workplace, but has also introduced significant security vulnerabilities as well, especially for organizations not using encryption or simply using standard WEP, which basically opens the network to any outsider. Many articles have been written about WLAN security best practices, but in short, if WLAN is being used, it MUST use strong wireless encryption and authentication such as WPA or 802.11i.

What to look for:

- For IPsec applications (sending data over the Internet, for example), make sure that the security appliance supports manual and automatic key (IKE) key exchanges, uses either 3DES or AES encryption, and uses MD5 or SHA-1 authentication.
- Make sure the appliance supports IPsec NAT traversal to ensure the VPN can operate in NAT environments.

Untangle's Next Generation Firewall meets all of the criteria on this list.

ABOUT UNTANGLE

Untangle, a network software and appliance company, provides the most complete multi-function firewall and Internet management application suite available today. Designed to meet the network policy demands of organizations large and small, Untangle's award-winning software now ships on easy-to-deploy appliances. Untangle's proven network software solutions are installed in nearly 40,000 organizations, protecting more than 2 million people and their computers. With its try-before-you-buy approach, Untangle enables organizations to take control of their network within minutes and at no risk.

For sales information, please contact us by phone in the US at +1 (866) 233-2296 or via e-mail at sales@untangle.com.

Untangle, Inc.
100 W. San Fernando St., Ste. 565.
San Jose, CA 95113
www.untangle.com