



Simply better network security.™

C O N T E N T

HIPPA Compliance Overview

Administrative Safeguards

Security Safeguards

Summary

www.esoft.com

▣ **White Paper: Ensuring HIPAA Compliance by
Implementing the Right Security Strategy**

HIPAA Compliance

It's a weekly occurrence at eSoft: a frantic IT manager gets notice through a security audit that they are non-compliant with HIPAA as it relates to handling patient data in electronic form (EPI - Electronic Protected Health Information, in HIPAA parlance). "But we JUST bought a new firewall from another vendor that does Intrusion Prevention and VPN, so we should have been OK... right?" Maybe and maybe not.

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 complicated topics. While healthcare industry IT managers may be security savvy, the problem is that HIPAA regulations dictate what CAN NOT happen with patient information-not what to do or how to do it. This is one of the most prolific criticisms of HIPAA in general.

So how does an IT manager know if they are covered in the face of a HIPAA audit? And how does the IT manager read a security product datasheet to assess whether a potential security solution will ensure compliance? The sections below extract 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 (Section 164.308)

164.308(a)(5)(ii)(B) - Protection From Malicious Software

HIPAA Text: "[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: (1) Virus and Worm protection through Gateway and Desktop Anti-virus systems (contrary to what many believe, AV systems do little to stop Trojans); (2) Trojan identification and mitigation, as well as FTP, IM and P2P threat mitigation through Intrusion Prevention (IPS) systems ; and (3) 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 Anti-Virus 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 (beware of firewalls that claim Intrusion Prevention but only protect against DoS attacks) and Gateway Anti-Virus services.
- Make sure that the solution's security services provide regular updates of signature files (e.g. every 30 minutes) 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'.
- Anti-Spyware would be optional for this standard, but it will be needed later on.
- **eSoft solutions meet all of the criteria on this list, including Anti-Spyware.**

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.
 - For Intrusion Prevention, make sure that it is an IPS system, rather than an IDS (Intrusion Detection) system.
- For the firewall, make sure it protects against at least the top 50 well-known DoS and DDoS attacks.
- Make sure the security device logs all attempted attacks, as well as steps the device takes to mitigate the attack. This will be hard to determine from a datasheet, so be sure to ask the vendor for sample logs.
- **eSoft solutions meet all of the criteria on this list.**

Security Safeguards (Section 164.312)

164.312(a)(1) - Access Control

"Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)"

In general, this is more of a Server-side requirement, but assuming the organization is using some form of RADIUS or LDAP authentication and 'rights management' system, the security infrastructure can have a tremendous impact.

Another helpful tool for enforcing information access is Email Content Filtering. In this type of system, the administrator would enter keywords or regular expressions (matching sequences) that would allow outgoing emails to be scanned for signs of inappropriate content. For instance, the administrator could set up a regular expression string to search for patient ID numbers (such as `"*PAT-[0-7]*-*****"`) and scan all outbound non-encrypted emails that would otherwise inappropriately send out confidential, HIPAA-protected content.

What to look for:

- Make sure that the security device supports your native form of authentication (such as RADIUS or LDAP).
- Make sure that for web-based applications, the device supports Transparent Authentication (TA), which is critical for users who hop around to different secure applications or to different areas of the same application. Without TA, the user will have to enter username and password information each end every time they make a jump.
- Ensure that the system supports Email Content Filtering with both keyword, and regular expression string matches. There should also be a quarantine for forensic analysis.
- eSoft solutions meet all of the criteria on this list.

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. A large number of HIPAA violations stem from weak encryption, lack of encryption, or misuse of encryption. Any time PHI is sent outside of 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. According to Taraboletti, "While it is not typically required to store data-at-rest in an encrypted format, transmission of data to external entities or locations over a public network MUST be strongly encrypted and users authenticated."

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.
- eSoft solutions meet all of the criteria on this list.

164.312(b) - Audit Controls

"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

It is important to be able to audit data records and make corrections. The old adage "If you cannot measure it, you cannot manage it" applies here. Because documentation lies at the heart of the HIPAA rules, we would also say, if you can't log it, you can't document it. In addition, any detailed security/IT audit begins with the log files. If you prefer, think of the "black box" on major airliners that record and track flight. You never hear about them unless there is a crash. While audit reports are important, the security appliance is also a necessary tool for capturing critical event data that support, and feed into security audits.

What to look for:

- Again, make sure the security device logs all attempted attacks, as well as steps the device takes to mitigate the attack. This will be hard to determine from a datasheet, so make sure to specifically ask the vendor.
- Confirm that the security device shows enough 'at-a-glance' information (and sends appropriate alerts) so that the IT manager is immediately aware of any anomalous activity. eSoft's ThreatMonitor is a good example of this type of tool.
- **eSoft solutions meet these requirements.**

164.312(c)(1) - Integrity

"Implement policies and procedures to protect electronic protected health information from improper alteration or destruction."

Under this standard, there is one sub-specification which must be addressed by network security:

164.312(c)(2) - Mechanism to Authenticate EPHI

"Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner."

This standard applies to data transmitted both internally and externally. Unfortunately, there are many "degrees of solution" to meet this standard, ranging from simple file checksums and use of digital signatures in email, to full anomaly-detection and file protection programs. By implementing Intrusion Prevention, Email Anti-Virus and Anti-Spyware in addition to use of digital signatures for email, the standard should be easily met.

What to look for:

- On the security device, support for packet-based (real-time) Intrusion Prevention, and proxy/file-based AV scanning is critical. This will ensure file and attachment integrity, while also providing detection of anomalous behavior aimed at altering information.
- **eSoft solutions meet this requirement.**

164.312(e) - Transmission Security

"Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."

This standard has two sub-specifications that must be addressed by network security:

164.312(e)(2)(i) - Integrity Controls

"Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of."

This is a critical standard of HIPAA. Because there are many ways of transmitting data, each must be addressed individually.

- For Email, the Email Content Filtering application described in "164.312(a)(1) - Access Control" will help prevent protected data from leaving the network, while use of digital signatures will ensure that senders are truly who they say they are. Digital checksums are built into most applications, so there should not be much to do there.
- For Instant Messaging, most Intrusion Prevention or Web Filtering applications provide simple mechanisms for turning off access to these applications.
- For FTP or other protocols, it is critical that a filtering application be in place that intercepts (or 'proxies') all transmissions to ensure that they are well-formed, and are sent/received by appropriate parties.

What to look for:

- Ensure that the security device performs full proxying for both SMTP as well as POP3 (if using hosted email) protocols, and that it provides Spam Filtering (DNS-RBL, Bayesian and SPF are critical) and Email Content Filtering (with regular expression matching, as well as quarantine functions).
- Make sure that the IPS or Web Filter application has settings to block all major Instant Messaging applications (AIM, ICQ, MSN Messenger and Yahoo Messenger). This is an area where there will be fewer and fewer integrated solutions that provide all of these services. Devices like the eSoft ThreatWall and InstaGate are designed to provide all of these 'deep packet' security services in one appliance, where other market solutions tend to be 'point solutions,' performing one or a few of these functions.
- **eSoft solutions meet all of these requirements.**

164.312(e)(2)(ii) - Encryption

"Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."

This functionality was described fully in the "164.312(a)(2)(iv) - Encryption and Decryption" section under Access Control, above.

Summary

When considering how the perimeter network security appliance can help ensure HIPAA compliance, a few clear trends emerge. First, there needs to be core Firewall and IPSec VPN functionality, where the Firewall provides NAT and basic security functions, as well as protection against well-known DoS attacks, and where the VPN provides strong encryption and authentication functionality for data in transit. Second, there needs to be strong email controls in the form of Anti-Spam (which will reduce risk due to Phishing attacks) and Email Content Filtering (which will help prevent protected data from inadvertently being sent outside the network). Third, both Desktop and Gateway Anti-Virus systems must be in place to prevent Viruses and Worms from altering and/or destroying data. Fourth, a Web Filtering application should be in place to prevent users from accessing known Spyware and hacker sites, and also to monitor and enforce employee Internet usage (this can greatly enhance workforce productivity, as well). Finally, an Intrusion Prevention system must be in place that constantly scans the network for signs of anomalous behavior, for signs of server and database attacks, and most importantly to deny access to risky IM and peer-to-peer file-sharing applications.

With HIPAA, the penalties can be steep, so indeed "an ounce of prevention is worth a pound of cure."

The problem is that not all security solutions are created equal. The prudent IT manager must ask vendors a lot of questions, and they must ask all the right questions. This white paper should serve as guide to help you determine what to ask vendors and what solutions will help you achieve HIPAA compliance.