



eEye Digital Security®

Attaining HIPAA Compliance with Retina® Vulnerability Assessment Technology



Attaining HIPAA Compliance

with Retina Vulnerability Assessment Technology

Utilizing Retina, eEye's vulnerability assessment and remediation solution handles the complete process.

Overview

The final privacy rules for securing electronic health care became effective April 14th, 2003. These regulations require health care companies to develop, implement, and document the measures they take to ensure that health information remains secure under the Health Insurance Portability and Accountability Act (HIPAA). HIPAA is intended to protect and simplify the exchange of health care data nationwide. Large health-care organizations will have until April 2005 to fully comply, while smaller entities will have until April 2006. The complete HIPAA information can be found at: <http://www.aspe.hhs.gov/admsimp/>

Now federal law, compliance with HIPAA is mandatory and violators face up to \$250,000 in fines and jail time of up to 10 years. HIPAA regulations are intended to protect such data as a patient's medical records and personal health care information. HIPAA affects organizations that transmit protected health information in electronic form (e.g. health plans, health care clearinghouses, and health care providers).

The law maintains that health care organizations implement a wide variety of safeguards and security best-practices in order to adequately protect customer data. Full compliance requires that these entities understand the threats and liabilities and take proactive measures to maintain reasonable and appropriate safeguards in three areas: administrative, physical, and technical. This document details the process needed to achieve compliance and breaks down the specific areas of HIPAA where eEye's Retina Network Security Scanner plays a pivotal role.

HIPAA & Retina Enterprise Edition

There are several areas in HIPAA where eEye's vulnerability assessment solution is key to attaining compliance. The sections include: Title II (Preventing Health Care Fraud and Abuse), Subtitle F (Administrative Simplification), Section 262, and Subsection 1173d (Security Standards for Health Information). As initially mentioned, Subsection 1173d contains the three security standards categories that are critical: administrative, physical, and technical. The final ruling on compliance requires all entities subject to HIPAA standards "to periodically conduct an evaluation of their security safeguards to demonstrate and document their compliance with the entity's security policy and the requirements of this subpart."

In terms of evaluation frequency, the regulations state that "covered entities must assess the need for a new evaluation based on changes to their security environment since their last evaluation, for example, new technology adopted or responses to newly recognized risks to the security of their information." HIPAA regulations also point out, "it is important to recognize that security is not a product, but is an ongoing, dynamic process." eEye's Retina Enterprise Edition automates and fulfills these process-oriented safeguard requirements for entities of all sizes. It is important to recognize the significance of the word "process" from the HIPAA regulations as it pertains to security within an organization. A computer security audit is a systematic, measurable technical assessment of how the entity's security policy is employed. Security audits do not take place in a vacuum and are part of the on-going methodology of defining, maintaining, and improving effective security throughout the organization. Following an established vulnerability assessment and remediation process is a proven approach to attaining HIPAA network security compliance.



Attaining HIPAA Compliance

with Retina Vulnerability Assessment Technology

Utilizing Retina, eEye's vulnerability assessment and remediation solution handles the complete process.

Six Steps of Vulnerability Assessment & Remediation

By using eEye's vulnerability assessment solution, Retina can identify the asset and identify risks and vulnerabilities, through the review and remediation stage, to final verification of fixes. Eye's complete Enterprise Vulnerability Assessment solution incorporates Retina and a sophisticated events management system to manage the entire process and minimizes resources needed to undertake this critical security initiative.

Step 1: Identify all network assets – discover functions wired and wireless

- a. Determine the existence and relative value of networked assets
- b. Create logical asset groupings
 - i. Separate revenue generating and application assets
 - ii. Separate desktops from mobile devices
 - iii. Group by business unit and location
 - iv. Measure the level of risk posed to critical processes and services
- c. Quickly identify high risk locations
 - i. Establish priorities and Rogue Devices

Step 2: Assess Security Risks – Scan for patches, vulnerabilities, setting and web application flaws

- a. Research audits
- b. SANS 20 Checks
- c. Secure configuration audits
- d. Policy violations
- e. Vendor disclosed audits
- f. Custom audits
- g. Device, user or other audits

Step 3: Mitigate existing security risks

- a. Remediate business critical applications using detail instructions and references
- b. Options to rescan and validate vulnerabilities
- c. Monitor remediation progress in the form of tasks and ticketing
- d. Analyze and adapt strategy to eliminate future security exposures
- e. Create custom rules to protect against specific threats and manage compliancy

Step 4: Prevent future security risks

- a. Protect against “methods of attack”
 - i. Zero-Day prevention
 - ii. Intrusion prevention
 - iii. Application and system firewall
 - iv. Policy enforcement
 - v. Virus, spyware, and phishing protection
 - vi. Vulnerability assessment agent
- b. Continuously protect and mitigate security risks for all devices
- c. Enforce corporate policy
- d. No signatures, no “learning mode”
- e. Single console management and reporting
- f. Recognized as the best protection for the end point

Attaining HIPAA Compliance

with Retina Vulnerability Assessment Technology

Utilizing Retina, eEye's vulnerability assessment and remediation solution handles the complete process.

Step 5: Manage and monitor risk

- a. Comprehensive third party integration
- b. Cisco NAC Game server integration
- c. Change device policy on the fly
- d. Alerting through:
 - i. Email, SNMP, Syslog, Windows Events

Step 6: Report on risk status

- a. After step two:
 - i. Severity of audit violation
 - ii. PCI compliance
 - iii. Grouping by asset, vulnerability, locations, etc.
 - iv. Most vulnerable hosts
 - v. Vulnerabilities by category
 - vi. Open ports and services
 - vii. Export data to a variety of formats
- b. Accurate and actionable report in your needed format
- c. Reporting by Region, business group, application, compliance

Achieving HIPAA Compliance with Retina

Below are the applicable areas where Retina is instrumental in attaining compliance – particular in the areas of administrative and technical initiatives since the physical safeguards that are nontechnical do not apply.

Administrative Safeguards

Security Management Process [Standard: (a)(1)(i)]

"Implement policies and procedures to prevent, detect, contain, and correct security violations."

This is the core strength of eEye's vulnerability assessment solution. Retina Enterprise Edition is a complete, automated system that performs non-intrusive audits to prevent, detect, contain, and correct security violations.

Evaluation [Standard: (a)(8)]

"Perform a periodic technical and non-technical evaluation based initially upon the standards implemented under this rule and subsequently, in response to environmental operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart."

Regular, scheduled vulnerability assessment audits can be performed by Retina, fulfilling this ongoing requirement for the entire network and verifying that any changes in the network have not created exposure.

Attaining HIPAA Compliance

with Retina Vulnerability Assessment Technology

Utilizing Retina, eEye's vulnerability assessment and remediation solution handles the complete process.

Technical Safeguards

Security Management Process - Risk Analysis [(a)(1)(ii)(A)]

"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities of the confidentiality, integrity, and availability of electronic protected health information held by the covered entity." Required implementation specification: (a)(1)(ii)(A).

Retina is one of the leading network vulnerability assessment scanner. Its database of vulnerability checks is the most accurate and comprehensive. Retina utilizes advanced technology to quickly and accurately test the strength of the entire network and reports on weaknesses with detailed remediation instructions.



Security Management Process - Risk Management [(a)(1)(ii)(B)]

"Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a)." Required implementation specification: (a)(1)(ii)(B).

Retina provides instant vulnerability information, which can be sorted in a variety of ways, including risk-level. For large organizations, Retina is the core of eEye's Enterprise Vulnerability Assessment solution that enables entities to compile vulnerability reports and automate the remediation management process for the entire organization - worldwide.

Security Management Process - Information System Activity Review [(a)(1)(ii)(D)]

"Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." Required specification: (a)(1)(ii)(D).

Retina automatically documents all incidents and effects of performed audits.

Security Incident Procedures [(a)(6)(i)]

"Implement policies and procedures to address security incidents." Standard: (a)(6)(i)

Vulnerability assessment audits performed by Retina provide the required data to implement and change security policies as appropriate to fortify the strength of the network.

Security Incident Procedures - Response and Reporting [(a)(6)(ii)]

"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." Required implementation specification: (a)(6)(ii).

Retina is one of the leading network vulnerability assessment scanner. It's database of vulnerability checks is the most accurate and comprehensive. Retina utilizes advanced technology to quickly and accurately test the strength of the entire network and reports on weaknesses with detailed corrective action instructions. All corrective actions can be immediately tested by running a follow-up scan to assure that corrective measures were properly followed to secure the entity.

Attaining HIPAA Compliance

with Retina Vulnerability Assessment Technology

Utilizing Retina, eEye's vulnerability assessment and remediation solution handles the complete process.

Technical Safeguards con't.

Business Associate Contracts and Other Arrangements [(b)(1) and (b)(4)]

"[An entity] may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances... that the business associate will appropriately safeguard the information." Standard (b)(1)

"Document the satisfactory assurances required... through a written contract or other arrangement with the business associate that meets the applicable requirements..." Required implementation specification: (b)(4)

Retina provides complete reports that can be used by the entity to assure compliance. Furthermore, Retina can be used by business associates to test their own security measures and assure that their networks are safe for creating, receiving, maintaining, or transmitting health information.

About eEye Digital Security

eEye Digital Security is pioneering a new class of security products integrated threat management. This next-generation of security detects vulnerabilities and threats, prevents intrusions, protects all of an enterprise's key computing resources, from endpoints to network assets to web sites and web applications, all while providing a centralized point of security management and network visibility. eEye's research team is consistently the first to identify new threats in the wild, and our products leverage that research to deliver on the goal of making network security as easy to use and reliable as networking itself. Founded in 1998 and headquartered in Orange County, California, eEye Digital Security protects more than 9,000 corporate and government organizations worldwide, including half of the Fortune 100. For more information, please visit www.eEye.com



eEye Digital Security®

To learn more, please visit www.eeye.com
or call 866.282.8276

