



eEye Digital Security®

What Every CIO Needs To Know About HIPAA Compliance



What Every CIO Needs To Know

About HIPAA Compliance

Unquestionably, the most critical phase in the entire vulnerability and remediation process involves properly auditing an entire network for vulnerabilities.

Executive Summary

The final privacy rules for securing electronic health care became effective in 2003. These regulations require healthcare 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 healthcare data nationwide. As of April 2006, all healthcare organizations are required to comply. The complete HIPAA information can be found at: <http://www.cms.hhs.gov/HIPAAGenInfo/>

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 healthcare information. HIPAA affects organizations that transmit protected health information in electronic form (e.g. health plans, healthcare clearinghouses and healthcare providers). The law maintains that healthcare 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® Network Security Scanner

There are several areas of HIPAA where eEye's vulnerability assessment solution is key to attaining compliance. These 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 or family of solutions 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.

What Every CIO Needs To Know

About HIPAA Compliance

Unquestionably, the most critical phase in the entire vulnerability and remediation process involves properly auditing an entire network for vulnerabilities.

Vulnerability Assessment & Remediation

eEye's vulnerability assessment solution incorporates Retina and a sophisticated events management system to manage the entire process and minimizes the resources needed to undertake this critical security initiative.

Phase 1: Discovery & Auditing

In order for organizations to assess their networks, it is important to understand the digital assets that make up the network. The first step in the vulnerability assessment and remediation process is asset identification. Though elementary, the Discovery Phase is an important first step in understanding the devices on a network. Retina quickly identifies and maps all of these elements in a centralized database.

Unquestionably, the most critical phase in the entire vulnerability and remediation process involves properly auditing an entire network for vulnerabilities. Retina is recognized as the leader in terms of its comprehensive auditing capabilities and unparalleled speed, accuracy and ease of use. With thousands of Retina scanners deployed worldwide, Retina has become the industry's most effective security auditing product.

Phase 2: Delegate & Remediate

Upon discovery of network issues, the task of assigning vulnerabilities for remediation can be simplified with an automated solution that incorporates a security events management system. eEye's Enterprise Vulnerability Assessment solution is designed for large, distributed enterprises with expansive networks that must be protected. For smaller organizations, the stand-alone capabilities within Retina meet the delegation needs of IT and network security personnel.

The Remediation Phase encompasses the "fixing" of the issue. eEye's technology provides hands-on fixes that resolve issues correctly - the first time. Detailed remediation instructions guide administrators through the process of correcting network vulnerabilities before an attacker can compromise them. After a patch or fix has been applied, a follow-up Retina scan serves as verification that the issue has been addressed and corrected.

Phase 3: Report & Adapt

Reporting, trend analysis, policy settings and resource management are all part of the Report & Adapt Phase of the vulnerability assessment and remediation management process. With HIPAA, this stage provides the necessary document to prove that the proper security measures are being completed on a regular, ongoing basis.

With proper auditing tools like Retina Enterprise, the unification of process and technology is simplified. Most importantly, implementing eEye's solution yields results and compliance for entities of all sizes that are subject to HIPAA regulations.

Achieving HIPAA Compliance with Retina

The following are the applicable areas where Retina is instrumental in attaining compliance - particularly in the areas of administrative and technical initiatives (physical safeguards that are non-technical do not apply for these purposes).

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 is a complete, automated system that performs non-intrusive audits to prevent, detect, contain, and correct security violations.

What Every CIO Needs To Know

About HIPAA Compliance

Unquestionably, the most critical phase in the entire vulnerability and remediation process involves properly auditing an entire network for vulnerabilities.

Administrative Safeguards con't.

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 or 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.

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 the industry's #1 rated 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.





eEye Digital Security®

What Every CIO Needs To Know

About HIPAA Compliance

Unquestionably, the most critical phase in the entire vulnerability and remediation process involves properly auditing an entire network for vulnerabilities.

Technical Safeguards Con't.

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 the industry's #1 rated 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.

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.

Conclusion

As with any IT project, working toward certifying compliance for regulations such as HIPAA must begin with a foundation in the organization's business and technical requirements, as there is no single 'magic bullet' that ensures compliance. Defining the vulnerability management criteria that are most critical and the tools to ensure those criteria are met is the right process for any ongoing compliance project.

About eEye Digital Security

Since 1998, eEye Digital Security has made vulnerability management simpler, less expensive and more effective by providing the only unified vulnerability and compliance management solution that integrates assessment, mitigation and protection into a complete offering. With a proven history of innovation, eEye has consistently been the first to uncover critical vulnerabilities and prevent their exploit. eEye leverages its world-renowned research to create award-winning solutions that strategically secure critical IT assets and the data they hold. Thousands of mid-to-large-size private-sector and government organizations, including some of the most complex IT environments in the world, rely on eEye solutions to protect against the latest known, unknown and zero-day vulnerabilities. For more information, please visit www.eeye.com

To learn more, please visit www.eeye.com

or call 866.282.8276