QUALYS®

VULNERABILITY MANAGEMENT FOR HIPAA COMPLIANCE

HIPAA Defined

HIPAA is U.S. Public Law 104-191 – the Health Insurance Portability and Accountability Act of 1996. Congress created the Act to improve health care enabled by the nation's health plans and providers. The Department of Health and Human Services mandates standards-based implementations of HIPAA by all health care organizations that create, store or transmit electronic protected health information. Non-compliance can trigger various civil penalties, including fines and/or imprisonment.

Digital Security Is Part of the HIPAA Process

Security is a crucial part of Administrative Simplification rules under Title II of HIPAA, which aim to protect the confidentiality, integrity and availability of electronic protected health information. The Department states, "[It] is important to recognize that security is not a one time project, but rather an ongoing, dynamic process." HIPAA therefore requires security-related processes, many of which are often better implemented with technology. HIPAA regulations do not mandate particular security technologies. Instead, they specify a set of principles for guiding technology choices – principles that mirror those underpinning the on demand QualysGuard vulnerability management "software-as-a-service."

QualysGuard Meets Key HIPAA Compliance Rules

The QualysGuard vulnerability management and policy compliance solution meets key security technology auditing requirements detailed in the Department's "Health Insurance Reform: Security Standards," Final Rule 45 CFR Part 164.308 (see back page for details). QualysGuard fulfills key Administrative Safeguards for evaluation, security management, security incident procedures, training, and security assurance requirements of business associate contracts.

Automation Makes Compliance Easier and Cost Effective

As an on demand web service, QualysGuard enables immediate compliance with key HIPAA security regulations by allowing subscribers to automatically discover and manage all devices and applications on the network, identify and remediate network security vulnerabilities, measure and manage overall security exposure and risk, and ensure compliance with internal and external policies for HIPAA.

> *"QualysGuard vulnerability management is an essential part of our strategy for protecting confidential patient information in accordance with HIPAA regulations."*
>
> Matthew Economou,
> Security Systems Analyst
> **Cincinnati Children's Hospital Medical Center**

> *"QualysGuard is an integral part of our security policies and practices. It streamlines a variety of complex auditing and testing procedures such as identifying devices, finding vulnerabilities and assisting in the repair process. Without having to add more technical staffers, the automation of security audits helps us quickly meet most of the key administrative procedures as outlined by HIPAA."*
>
> George Zimmerman,
> Internet Administrator
> **St. Peter's Health Care Services**

ON DEMAND SECURITY

Vulnerability Management for HIPAA Compliance

QualysGuard capabilities directly address many key Administrative Safeguards. The matrix quotes HIPAA security standards and implementation specifications at 45 CFR Part 164.308, and associates each with QualysGuard capabilities.

HIPAA REQUIREMENTS	QUALYSGUARD CAPABILITIES
Evaluation – "Perform a periodic technical and nontechnical 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." Standard: (a)(8)	On demand vulnerability management with QualysGuard automatically fulfill this ongoing HIPAA security requirement by testing and documenting security capabilities before and after installation and maintenance of systems or applications
Security Management Process – "Implement policies and procedures to prevent, detect, contain, and correct security violations." Standard: (a)(1)(i)	QualysGuard provides a complete, automated system for security audits and vulnerability management
Security Management Process (Risk Analysis) – "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity. Required implementation specification: (a)(1)(ii)(A)	QualysGuard uses the largest database of vulnerability tests and intelligent scanning technology to ensure comprehensive, accurate security audits
Security Management Process (Risk Management) – "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)	Automated, comprehensive reports from QualysGuard provide instant assessment of risks and priorities for vulnerability remediation
Security Management Process (Information System Activity Review) – "Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. Required implementation specification: (a)(1)(ii)(D)	QualysGuard automatically documents all security incidents and subsequent effects of vulnerability remediation
Security Incident Procedures – "Implement policies and procedures to address security incidents." Standard: (a)(6)(i)	Security audit assessments provided by QualysGuard provide hard data for conceiving, implementing and managing security policies
Security Incident Procedures (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." Required implementation specification: (a)(6)(ii)	QualysGuard scans for vulnerabilities using the industry's largest and most up-to-date KnowledgeBase of known security issues, and provides verified fixes with one mouse click
Security Awareness and Training – "Implement a security awareness and training program for all members of its workforce (including management)." Addressable standard: (a)(5)(i)	Security data revealed by powerful QualysGuard reporting capabilities cuts out guesswork in teaching staff and management about the real-world protection of their network
Business Associate Contracts and Other Arrangements – "A covered 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)	Security data revealed by powerful QualysGuard reporting capabilities cuts out guesswork in teaching staff and management about the real-world protection of their network

QUALYS®

USA – Qualys, Inc.
1600 Bridge Parkway
Redwood Shores
CA 94065
T: 1 (650) 801 6100
sales@qualys.com

UK – Qualys, Ltd.
224 Berwick Avenue
Slough, Berkshire
SL1 4QT
T: +44 (0) 1753 872101

Germany – Qualys GmbH
München Airport
Terminalstrasse Mitte 18
85356 München
T: +49 (0) 89 97007 146

France – Qualys Technologies
Maison de la Défense
7 Place de la Défense
92400 Courbevoie
T: +33 (0) 1 41 97 35 70

ON DEMAND SECURITY