



QUALYS™

ON DEMAND
VULNERABILITY MANAGEMENT



CASE STUDY: Geisinger Health System— Bringing HIPAA Compliance to an Electronic Medical Record System

Geisinger Overview

Scope: regional (Pennsylvania)

Business: provides healthcare for 2.3 million people in 38 counties

Size: 8,500+ employees including physicians, 42 primary care sites, 56 clinics, \$2.3 billion in annual revenue, \$68 million spent on electronic medical records (EMR) since 1995

Web site: www.geisinger.org

The Geisinger Story

Business Problem

Protect the security and integrity of EMR accessed online by clinical providers and patients, and comply with HIPAA security regulations.

Operational Hurdle

Providing and verifying security for a complex system of several patient and clinical provider Web portals and 435+ network applications, approximately 70 of which feed data to the EMR system.

Solution

Geisinger used a Web service and internal network appliances from Qualys to automatically find vulnerabilities and document remediation in its network supporting the EMR system.

Geisinger®

The Geisinger Health System was created in 1915 at the bequest of 85-year-old Abigail A. Geisinger.

Her founding instructions were: "Make my hospital right; make it the best." Geisinger's bold vision has resulted in one of the largest rural healthcare facilities in the United States. Last year physician-led Geisinger hosted more than 58,000 visits to emergency rooms, performed more than 27,000 surgeries and received patients from more than 1,900 life flight helicopter sorties. Geisinger is one of the largest group medical practices in Pennsylvania.

Geisinger is also one of the most technically advanced healthcare institutions, providing instant Web access to healthcare records and medical information for thousands of employees and physicians, and more than two million patients in Pennsylvania. Since 1995, Geisinger has invested more than \$68 million to create one of the largest Electronic Medical Records systems in the country. The networked IT operating environment includes more than 500 servers and 9,000 PCs.

Like other healthcare institutions, Geisinger is required to verify compliance with the Health Information Portability and Accountability Act (HIPAA) and its accompanying regulations. In addition to

developing policies and procedures for ensuring compliance with transaction and code sets, patient record privacy and national identifiers, Geisinger needed a practical, economic way to audit the security of its network, quickly remediate vulnerabilities and verify security to external auditors. In 2003, Geisinger turned to Qualys for help with the audit, remediation and documentation of its related network security efforts.

Geisinger Chooses the Qualys Vulnerability Management Solution for HIPAA Compliance

Strengthening vulnerability management capabilities was a key motivation as Geisinger developed a HIPAA compliance program, according to Jaime Chanaga, Chief Information Security officer at the healthcare provider. Chanaga was hired by Geisinger partly to manage development and implementation of new system-wide policies, standards, guidelines and procedures for safeguarding the organization's information resources in conjunction with HIPAA mandates.

"We especially wanted to ensure the privacy, confidentiality and security of electronic medical records for our patients," says Chanaga. "Geisinger operates portals for clinical providers and patients to access those records over the Web."

Geisinger's Mandates

- Audit security and document compliance with HIPAA
- Proactively identify, prioritize and remediate network vulnerabilities
- Protect security and integrity of electronic medical records and access systems

Why Geisinger Chose Qualys

- Automated on demand audits
- Instant risk assessment
- Comprehensive, accurate reports for HIPAA compliance
- Proactive, easy to use
- Exceptional value

Geisinger determined that its existing manual security auditing processes were not comprehensive and were too slow to protect the organization from exposure to new viruses and worms. Geisinger currently has about 435 applications on its network. Approximately 70 of these feed data to electronic medical records accessed through the two Web portals.

"From a practical perspective, it was clear we needed to automate system vulnerability security audits and get help speeding the remediation of system vulnerabilities," Chanaga says. Geisinger also needed a way to document security compliance with HIPAA.

An evaluation of market alternatives by the Information Security Office and the IT department led to Geisinger's choice of the Web-based QualysGuard vulnerability management service from Qualys, Inc.

QualysGuard Automates Security Audits and Vulnerability Management at Geisinger

QualysGuard automates the processes of vulnerability management for Geisinger—from host discovery and vulnerability assessment to on demand reporting and remediation tracking for vulnerabilities found on Geisinger's systems and networks.

Automation in QualysGuard allows Geisinger to do security audits and vulnerability management on demand. It eliminates the provider's former time-intensive manual audit processes, saving time and improving the accuracy of results. Automatically generated comprehensive security audit and vulnerability management reports are of special value for Geisinger. "Many organizations, including third party auditors, use QualysGuard reports to confirm HIPAA technical security compliance," says Chanaga.

Geisinger Economically Protects Its Electronic Medical Record Systems With QualysGuard

Automated processes built into QualysGuard help reduce the costs of vulnerability management as much as 90 percent for large, distributed organizations like Geisinger.

The provider currently does automated scans with QualysGuard on a weekly basis. As part of its multi-layered security program, Geisinger also uses other techniques and technologies such as network segmentation, intrusion prevention, firewalls and antivirus software.

Ultimately, the big value for Geisinger with QualysGuard is having the technical means to verify security for electronic patient records.

"QualysGuard helps us protect the security and integrity of our electronic medical record systems," says Chanaga. "Compliance with HIPAA regulations is important to our organization. Our patients value the best possible healthcare with the assurance that their personal health information stays confidential. QualysGuard helps us achieve those ends."

"QualysGuard reports are an excellent solution for documenting IT security controls and compliance with regulatory requirements."

"QualysGuard helps us protect the security and integrity of our systems supporting our electronic medical record systems."

Jaime Chanaga CISO, Geisinger