

A New Approach to Security & Compliance for Healthcare



nopsec.com | hello@nopsec.com

Table of Contents

Executive Summary	2
Cyber Threat Landscape For Healthcare	3
Greater Vulnerabilities in Data Security	4
Top Information Security Concerns	4
Addressing Security for Compliance	5
Cyber Security Compliance - Healthcare	6
Barriers to Security and Compliance	6
A New Approach For Security and Compliance	8
About NopSec	11

Executive Summary

In the battle against cybercrime, small healthcare organizations are in an unenviable spot. The good news is that compared to other sectors, breaches with data losses rank relatively low. The bad news is that the value of one record of electronic protected health information is worth about 10 times the value of a single payment card's account data. This big lure, coupled with a relatively immature cyber security posture, makes healthcare a sitting duck for new attacks – especially smaller organizations.

With limited budgets and internal expertise, small healthcare organizations struggle with using and managing a myriad of manual security tools that swamp and paralyze them with obscure, irrelevant data. But there's also an opportunity to take action and avoid a disastrous breach. And "disaster" can mean far more damage than penalties for non-compliance with HIPAA/HITECH. The new direction is to systematically assess vulnerabilities and distill the right data to make accurate, informed and timely decisions for precisely predicting and remediating threats. The security achieved by these steps also helps organizations to comply with laws and regulations, avoid related financial costs and penalties, and protect the brand.

This paper describes how smaller healthcare organizations can reach these objectives by gaining a deeper understanding of the cybersecurity regulatory landscape – and tailoring a cloud-based SaaS approach that automatically filters complex threat data and distills it into precise threat prediction for rapid remediation.

Cyber Threat Landscape For Healthcare

Previously, the \$1.7 trillion-in-revenue healthcare industry¹ has relatively avoided attention by data thieves. In 2014, Verizon reports the sector had just 6.6% of all breaches with confirmed data loss occurring in 20 business sectors. Sectors with significantly more breaches with confirmed data loss included accommodation, financial services, manufacturing, public, and retail².

But healthcare is emerging as a new lucrative target for data thieves. According to Reuters, the personally identifiable information in a medical healthcare record is worth 10 times more than a payment card record in the black market³. Exposure of electronic protected healthcare information (ePHI) stems from several factors⁴:

- Adoption of digital patient records and automation of clinical systems
- Use of antiquated electronic medical records (EMR) and clinical applications that do not operate securely
- Ease of distributing ePHI internally and externally
- Using systems with EMRs and ePHI on the same network used to browse the Internet
- Rising sophistication of cyber attacks

¹ See <http://www.statisticbrain.com/health-care-industry-statistics/>

² Verizon 2015 Data Breach Investigations Report, p. 3.

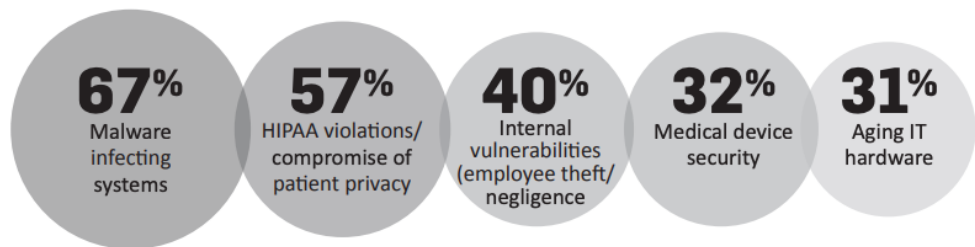
³ Caroline Humer and Jim Finkel, "Your Medical Record Is Worth More to Hackers than Your Credit Card" at <http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924>

⁴ Health Care and Cyber Security: Increasing Threats Require Increased Capabilities, KPMG Survey in 2015, p. 2

Greater Vulnerabilities in Data Security



Top Information Security Concerns



Source: KPMG

Specific areas of major vulnerability documented in breaches at healthcare organizations include miscellaneous errors committed by insiders and privilege abuse⁵. Cloud applications pose other risks when they contain ePHI, such as email/messaging, patient portal/PHR, billing and records, EMR/HER, health information exchange, and storage⁶. Healthcare organizations also face the onus of getting third party service providers to use strong security for HIPAA compliance.

HIPAA compliance is a pressing issue for healthcare organizations, not the least is the potential penalty of up to \$1.5 million for non-compliance⁷. While compliance does not

⁵ Verizon 2015 Data Breach Investigations Report, p. 34.

⁶ 2014 SANS Health Care Cybersecurity Survey, p. 8.

⁷ U.S. Department of Health & Human Services, HITECH Act Enforcement Interim Final Rule, Table 1.

guarantee security, it's a good starting point to measure the strength of deployed cyber defenses.

Addressing Security for Compliance





When you think about compliance, picture four general areas that may affect financial services: (1) laws and regulations, (2) standard frameworks, (3) audit guidelines, and (4) industry controlled regulations. Many financial services firms must address compliance requirements in all four areas (see chart below for examples).

To verify the deployment and ongoing maintenance of security controls and processes, security audits are mandatory for the healthcare industry. The audit bible is the U.S. Health and Human Services Office for Civil Rights HIPAA Audit Protocol⁸. For vulnerability management, healthcare organizations must document assessments of potential risks and vulnerabilities of ePHI. They must verify current security measures are sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. They must obtain satisfactory assurance from business associates that they will appropriately safeguard the information in accordance with HIPAA requirements. Organizations must document remediation responses and outcomes to security incidents. They also must periodically evaluate security safeguards and demonstrate and document compliance⁹.

⁸ See details in <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html>

⁹ See HHS OCR HIPAA Audit Protocol §164.308.

Cyber Security Compliance - Healthcare

Laws & Regulations 	HIPAA / HITECH – Privacy, security and enforcement rules in the <i>Health Insurance Portability and Accountability Act</i> and the follow on <i>Health Information Technology for Economic and Clinical Health Act</i> include administrative, physical and technical safeguards to protect electronic protected health information.
Standard Control Frameworks 	NIST – <i>The National Institute of Standards and Technology</i> specifies technical standards. HIPAA relies on NIST for the fine print of network and IT security specifications, such as NIST Special Publication 800-66, <i>An Introductory Resource Guide for Implementing the HIPAA Security Rule</i> . ISO/IEC – Multinational healthcare organizations often rely on the International Organization for Standardization and International Electrotechnical Commission <i>ISO/IEC 27002</i> guidelines for network and IT security. COBIT – <i>The Control Objectives for Information and Related Technology</i> framework to bridge the gap between security control requirements, technical issues and business risk. It's by the Information Systems Audit and Control Association (ISACA).
Audit Guidelines 	HHS – U.S. Department of Health and Human Services Office for Civil Rights HIPAA Audit Protocol is used to analyze processes, controls, and policies of a health care organization according to the HITECH Act audit mandate. AICPA – American Institute of Certified Public Accountants provides <i>Statements on Auditing Standards</i> , including network and IT security guidelines such as <i>Critical Security Audit Considerations</i> . Service providers to financial institutions often must contractually provide security certification with AICPA's <i>Statement on Standards for Attestation Engagements (SSAE) No. 16</i> (formerly SAS 70).
Industry Self-Regulations & Guidelines 	HITRUST – The Health Insurance Trust Alliance provides its Common Security Framework (CSF) addressing security and compliance by healthcare organizations. Many providers are now requiring CSF Certification by its business associates. PCI – The Payment Card Industry Security Standards Council's PCI Data Security Standard provides security requirements and guidelines for every entity that stores, transmits or processes payment cards.

Barriers to Security and Compliance

Compliance is the Number One driver to healthcare organizations for securing ePHI¹⁰. But the intent of compliance is not simply to push reports about passing a test. As healthcare organizations achieve ongoing compliance they will also establish the foundation of a more secure environment to protect ePHI. The key to staying ahead of new attacks is to quickly find and fix vulnerabilities.

¹⁰ 2014 SANS Health Care Cybersecurity Survey, p. 7.

The SANS survey notes almost a dozen drivers for securing ePHI. In addition to compliance, other top worries included the ability to respond to new or emerging threats, the ability to recover quickly from a breach incident,¹¹ and financial fallout from a breach such as reputational risk – which could trigger loss of customer trust and business, or even a lower institutional credit rating¹².

Clearly, healthcare organizations know they need to do more for securing ePHI. Just 53% of providers and 66% of payers consider themselves ready to defend against a cyber attack, according to KPMG. And 23% do not have a security operations center to identify and evaluate risks. Notably, 65% said they did not have enough resources for managing vendor security risks; 45% said the same for handling security incidents¹³.

In a survey by Ponemon Institute, half of all healthcare organizations “have little or no confidence in their ability to detect all patient data loss or theft.” The majority “fail to perform a risk assessment for security incidents, despite the federal mandate to do so.” Ponemon says the average cost of a data breach for a healthcare organization is more than \$2.1 million¹⁴. Ponemon says “the most-often reported root cause of a data breach is shifting from lost or stolen computing devices to criminal attacks.”

¹¹ 2014 SANS Health Care Cybersecurity Survey, p. 7.

¹² See “Cyberattacks Could Hurt Credit Ratings in Health Sector” at <http://www.ihealthbeat.org/articles/2015/11/30/report-cyberattacks-could-hurt-health-care-institutions-credit-ratings>.

¹³ Health Care and Cyber Security: Increasing Threats Require Increased Capabilities, KPMG Survey in 2015, p. 4, 6

¹⁴ Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2015 (sponsored by ID Experts), pp. 1-2.

Criminals often exploit vulnerabilities posed by emerging technologies as these may not be addressed by legacy security controls and processes. In just one example of mobile security, SANS healthcare survey respondents noted several mobile security concerns: lack of awareness about security policies; insecure/unprotected endpoints; lost or stolen devices; corrupt, hacked or malicious apps; insecure wireless use; and insecure web browsing¹⁵. Other relevant emerging issues include bring-your-own-device (BYOD), insecure public networks, and pass through attacks from vulnerabilities in IT used by business partners and suppliers.

A New Approach For Security and Compliance

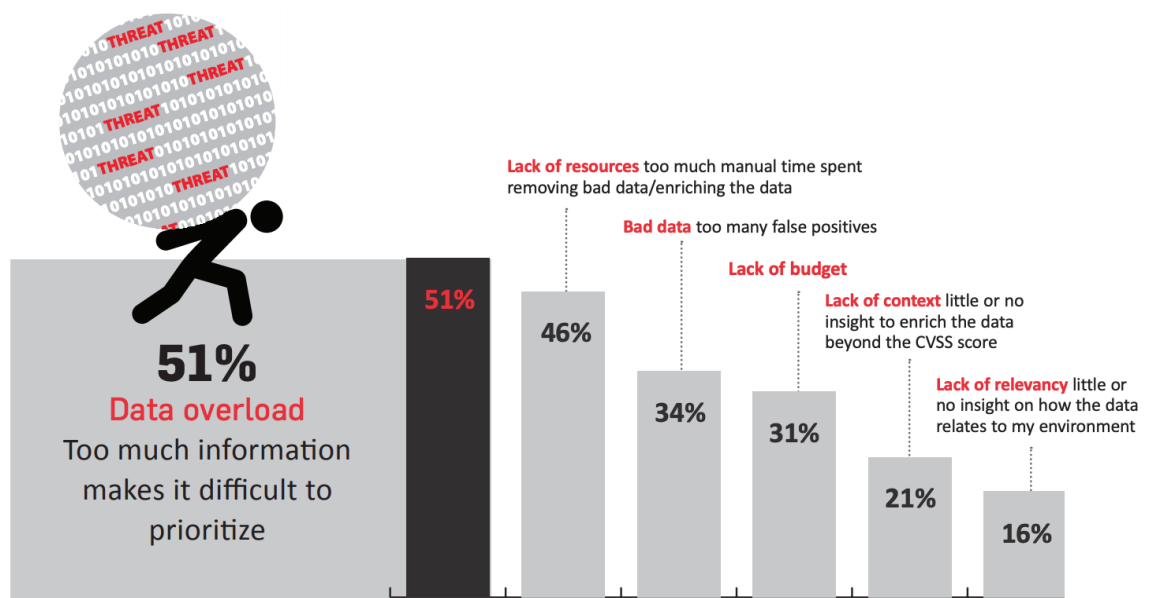
Small financial services firms struggle to fight sophisticated threats and securing emerging technologies such as mobile banking and payments. The security budgets are smaller. They also have less security expertise and fewer IT staff – who are swamped by alerts of hard-to-understand system and vulnerability data. Without priorities, remediation efforts are slow and less effective. This is where a cloud-based automated solution for continuous vulnerability management (VM) can help to acquire actionable intelligence. Done well, VM is an automatic, continuous process of identifying and prioritizing vulnerabilities, rapid remediation, and governance. Using a cloud solution makes it easy to buy, deploy and use VM.

¹⁵ 2014 SANS Health Care Cybersecurity Survey, p. 18.

Prioritization: An organization should prioritize vulnerabilities in order to know what to fix first. A cloud-based automated VM solution can eliminate labor-intensive tasks of prioritization. The solution must filter vulnerability scanning data from multiple sources to identify actual vulnerabilities and precisely predict threats. Regulatory and audit guidance prescribes a risk-based process that weighs vulnerabilities by business risk and likelihood of a breach. All this can be automated to save you time and improve accuracy of results.

Remediation: Workflow automation will help you accelerate the remediation process. Elements of remediation include ticket tracking, task management, patch deployment, and rescanning to verify successful fixes. It's essential for small financial services firms to synchronize communications with an automated system that coordinates all remediation activity. This helps provide siloed teams with the actionable information they need to work together on remediation.

Governance: Tracking vulnerability management and remediation results will help financial services firms to evaluate security efforts and improve security and compliance, a cloud-based automated solution for VM will simplify governance with customizable reports and well-presented data to inform technical staff, managers and executives of security posture.



Source: NopSec (2016 Outlook / Survey)

Find out how NopSec's Unified VRM can help you think like a hacker and stay ahead of the trends. Visit www.nopsec.com or email hello@nopsec.com for additional information or to request a demo.

About NopSec

NopSec operates with one mission: to help people make better decisions to reduce security risks. Our team is passionate about building technology to help customers simplify their work, manage security vulnerability risks effectively, and empower them to make more informed decisions. Our software-as-a-service approach to vulnerability risk management offers an intelligent solution to dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation.

NopSec helps security professionals simplify their work, effectively manage and prioritize vulnerabilities, and make better informed decisions.

NopSec's Unified VRM is an innovative threat and vulnerability management solution that addresses the need for better prioritization and remediation of security vulnerabilities in a single platform.

NopSec Inc. • www.nopsec.com • info@nopsec.com



