Architecting Security to Address Compliance for Healthcare Providers

What You Need to Know to Help Comply with HIPAA Omnibus, PCI DSS 3.0 and Meaningful Use

November, 2014
# Table of Contents

- Background .................................................................................................................................................. 3
  - State of Security in Healthcare .................................................................................................................. 3
  - Breaches on the Rise..................................................................................................................................... 4
- Regulatory Landscape ...................................................................................................................................... 6
  - HIPAA ......................................................................................................................................................... 6
  - HITECH ......................................................................................................................................................... 8
  - PCI DSS ......................................................................................................................................................... 10
  - HITRUST Common Security Framework ....................................................................................................... 10
- Improving Security and Meeting Compliance Needs with Trend Micro .......................................................... 12
Background

State of Security in Healthcare

Healthcare organizations often lack the financial and human resources required to implement comprehensive information security programs. Increasingly complex healthcare IT systems, medical devices containing software, mobile devices, patient portals, legacy systems, and aging infrastructures, all combine to make comprehensive security of the healthcare organization’s environment ever more challenging. As a further challenge, the information collected by healthcare organizations is valuable, creating a lucrative target for attackers. The lack of a comprehensive security program that addresses all of these areas often leads to data breaches.

In addition, healthcare organizations must comply with increasingly complex federal and state regulatory requirements related to the privacy and security of Protected Health Information (PHI). When the Department of Health and Human Services (HHS) or a covered entity receives a complaint, healthcare organizations are liable for the time and costs of an investigation, even if the complaint is not substantiated. Healthcare organizations often lack the financial resources to cover the cost of the investigations and penalties assessed for non-compliance.

As a result, many organizations focus on complying with the regulations instead of implementing comprehensive information security programs. However, complying with the regulations does not necessarily make an organization secure or immune from potential breaches.
Breaches on the Rise

With the increasing volume and complexity of regulatory requirements and the costs associated with disclosure after a breach, one might expect the healthcare industry to be fairly mature with respect to protecting PHI. Unfortunately, breach and benchmark data indicate otherwise.

Since the Breach Notification Rule went into effect September 2009, HHS received 930+ reports involving breaches of PHI affecting 500 or more individuals as of April 2014\(^1\). In addition, HHS received 114,000+ reports of breaches of PHI affecting less than 500 individuals.

- Theft and loss account for 58% of large breaches.
- Laptops and other portable storage devices account for 34% of large breaches.

A study conducted by the Ponemon Institute\(^2\) provides further insight into the causes of data breaches. According to the Ponemon study,

“Criminal attacks on healthcare organizations increased 100 percent since 2010. Insider negligence continues to be at the root of most data breaches reported in this study but a major challenge for healthcare organizations is addressing the criminal threat as shown in Figure 8. These types of attacks on sensitive data have increased 100 percent since the study was conducted in 2010 from 20 percent of organizations reporting criminal attacks to 40 percent of organizations in this year’s study”.

“Consistent with previous studies, the primary cause of breaches is a lost or stolen computing device (49 percent), which can be attributed in many cases to employee carelessness. This is followed by employee mistakes or unintentional actions (46 percent), and third-party snafus (41 percent)”.

---

1. Lessons Learned from Recent HIPAA Enforcement Actions, Breaches, and Audit, Iliana L. Peters, J.D., LL.M, April 23, 2014
2. Fourth Annual Benchmark Study on Patient Privacy and Data Security, Ponemon Institute, March, 2014
Verizon’s 2014 Data Breach Investigations Report shows similar causes of data breaches experienced by the healthcare industry:

- 46% involved theft or lost devices
- 15% involved insider misuse: unapproved or malicious use of organization resources
- 12% involved miscellaneous errors: unintentional actions directly compromised a security attribute of an information asset

Healthcare organizations that experience a breach are financially impacted by the cost of the actual notification, sending out letters, and associated costs like credit monitoring, forensic analysis, remediation and reputational damage. According to the Ponemon study,

“Data breaches continue to cost some healthcare organizations millions of dollars every year. While the cost can range from less than $10,000 to more than $1 million, we calculate that the average cost for the organizations represented in this year's benchmark study is approximately $2 million over a two-year period. This is down from $2.4 million in last year’s report as well as from the $2.2 million reported in 2011 and $2.1 million in 2010. Based on the experience of the healthcare organizations in this benchmark study, we believe the potential cost to the healthcare industry could be as much as $5.6 billion annually.”

In addition to the cost of a breach, the Office for Civil Rights (OCR), which is responsible for enforcing the HIPAA Rules, may also levy fines for HIPAA violations. State Attorneys General can also enforce the HIPAA Rules and levy additional fines on organizations.

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
<th>Violations of Identical Provision (per calendar year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A) Did Not Know</td>
<td>$100—$50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>(B) Reasonable Cause</td>
<td>$1,000—$500,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>(C)(i) Willful Neglect—Corrected</td>
<td>$10,000—$50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>(C)(i) Willful Neglect—Not Corrected</td>
<td>$50,000</td>
<td>$1.5 million</td>
</tr>
</tbody>
</table>

**HIPAA Penalties**

OCR fines can add up quickly as shown in the following chart.

<table>
<thead>
<tr>
<th>Covered Entity</th>
<th>2013 OCR Fine</th>
</tr>
</thead>
<tbody>
<tr>
<td>New York and Presbyterian Hospital (NYP) and Columbia University (CU)</td>
<td>$4,800,000</td>
</tr>
<tr>
<td>WellPoint Inc.</td>
<td>$1,700,000</td>
</tr>
<tr>
<td>Affinity Health Plan, Inc.</td>
<td>$1,215,780</td>
</tr>
<tr>
<td>Idaho State University</td>
<td>$400,000</td>
</tr>
<tr>
<td>Shasta Regional Medical Center</td>
<td>$275,000</td>
</tr>
<tr>
<td>Skagit County</td>
<td>$215,000</td>
</tr>
<tr>
<td>Adult &amp; Pediatric Dermatology, P.C.</td>
<td>$150,000</td>
</tr>
</tbody>
</table>

---

3 2014 Data Breach Investigations Report, Verizon
4 Lessons Learned from Recent HIPAA Enforcement Actions, Breaches, and Audit, Iliana L. Peters, J.D., LL.M, April 23, 2014
Healthcare organizations must implement comprehensive security programs in order to avoid data breaches and stiff financial penalties. In order to understand how to accomplish both goals, let’s first look at the regulatory landscape and then discuss additional measures to improve security.

**Regulatory Landscape**

Since the Health Insurance Portability and Accountability Act (HIPAA) was enacted on August 21, 1996, the healthcare industry has seen a steady stream of regulations such as the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) and the Data Breach Notification Rule of 2009. In addition, healthcare organizations who conduct credit card transactions must comply with the Payment Card Industry Data Security Standards (PCI DSS).

Covered entities and business associates must address the privacy and security of patients’ PHI by complying with HIPAA, HITECH and the Data Breach Notification Rule.

Covered Entities are defined by HIPAA as

> “Healthcare providers, clearinghouses and health plans that electronically transmit any health information in connection with transactions for which Health and Human Services (HHS) has adopted standards. Generally these standards are for billing, and payment for services or insurance coverage”\(^5\).

Business Associates are defined by HIPAA as

> “A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity”\(^6\).

Let’s look at each regulation in depth to see if there is any guidance on security.

**HIPAA**

Health Insurance Portability and Accountability Act of 1996

HIPAA was designed to improve the continuity of coverage and care services while simplifying the administration of healthcare. HIPAA established a set of national privacy and security standards for the protection of certain health information.

The HIPAA Privacy Rule, which went into effect in 2003, requires that healthcare organizations protect PHI and keep patient information confidential. PHI can only be accessed by authorized individuals on a need-to-know basis. In addition, HIPAA requires the development and adoption of standards to secure PHI while in the custody of covered entities, as well as in transit between covered entities and third-parties. These requirements became the foundation of the HIPAA Security Rule that went into effect in 2005.

Generally, the Security Rule requires a covered entity to:

- Ensure the confidentiality, integrity, and availability of all electronic PHI (ePHI) the covered entity creates, receives, maintains, or transmits.

---

\(^5\) 45 CFR § 160.103

\(^6\) 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e)
• Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
• Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.
• Ensure compliance by its workforce.

These protections are set forth as administrative, physical and technical safeguards described as follows:

• **Administrative Safeguards:** The Security Rule defines administrative safeguards as, “administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.”

• **Physical Safeguards:** The Security Rule defines physical safeguards as “physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.” The standards are another line of defense (adding to the Security Rule’s administrative and technical safeguards) for protecting EPHI.

• **Technical safeguards:** The Security Rule defines technical safeguards in § 164.304 as “the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.”

In order to achieve compliance with the HIPAA Security regulation, Meditology recommends covered entities follow the same basic approach, which at minimum includes:

1. Read the Security Rule.
   A covered entity should review all the standards and implementation specifications outlined in the Security Rule.

2. Perform a Risk Analysis of its current environment.

3. Develop an implementation plan.

4. Review the addressable implementation specifications.
   For each addressable implementation specification, a covered entity must determine if the implementation specification is reasonable and appropriate in its environment. A covered entity needs to consider a number of factors in making the decisions for each addressable implementation specification.

5. Determine security measures.
   A covered entity may use any security measures that allow it to reasonably and appropriately implement the standards and implementation specifications (see 45 CFR § 164.306(b), Flexibility of Approach).

6. Implement solutions.
   A covered entity must implement security measures and solutions that are reasonable and appropriate for the organization.

A covered entity must document its analysis, decisions and the rationale for its decisions.

8. Reassess periodically.

A covered entity must periodically review and update its security measures and documentation in response to environmental and operational changes that affect security of its ePHI.

HITECH
Health Information Technology for Economic and Clinical Health Act of 2009

HITECH was enacted as part of the American Recovery and Reinvestment Act (ARRA) to promote the adoption and meaningful use of health information technology. HITECH provided incentives for healthcare providers to make the transition from paper to electronic health records (EHR) systems and created opportunities for jobs related to the “meaningful use” of healthcare IT.

Subtitle D of the Act addresses the privacy and security concerns associated with the electronic transmission of health information, partly through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules. HITECH made numerous provisions of the Privacy and Security Rules expressly apply to business associates and their subcontractors.

HITECH also strengthens federal privacy and security laws to protect health information from misuse as the health care sector increases use of health IT.

Generally these changes include:

- Requiring that an individual receive notification if there is an unauthorized disclosure or use of their health information (see Breach Notification Rule).
- Expanding the scope of the HIPAA Rules to directly apply to entities that store, process or transmit PHI on behalf of providers and insurers.
- Requiring that providers obtain authorization from a patient to use their health information for certain marketing communications for which the covered entity receives remuneration.
- Providing the right to individuals to obtain their PHI in an electronic format.
- Explicitly prohibiting the sale of PHI without an authorization.
- Strengthening the enforcement of HIPAA by increasing penalties for violations and providing greater resources for enforcement and oversight activities.

Breach Notification Rule

HITECH also resulted in the modification of the HIPAA Privacy, Security and Enforcement Rules and created the Breach Notification Rule. The Breach Notification Final Rule became effective on September 23, 2013.

A breach is defined by the Rule as

“An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.”

Covered entities and business associates are only required to provide notification if the breach involves unsecured PHI:
“Unsecured PHI is defined as PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of an approved technology or methodology.”

There are certain exceptions to the current Rule whereby an organization does not need to provide notification for a breach of unsecured PHI, commonly referred to as “Safe Harbor.” Safe harbor is granted when either of the following is true:

- The patient information is encrypted and subsequently inaccessible by an unauthorized individual. Encryption systems must meet the NIST SP 800-111 “Guide to Storage Encryption Technologies for End User Devices” standard for stored data to be deemed secure.
- The patient information has been disposed of in a secure manner, such as degaussing hard drives or shredding paper records. Electronic media must be cleared, purged, or destroyed consistent with NIST SP 800-88 “Guidelines for Media Sanitization”.

An incident must be analyzed using a four step risk analysis to determine whether PHI has been compromised. The incident is presumed to be a breach unless the risk analysis reveals low probability that the PHI has been compromised. The risk analysis must be documented and retained to meet the covered entity’s burden of proof to demonstrate that unreported incidents did not rise to the level of a breach.

When a breach occurs, the organization has 60 days to notify the individuals whose information was involved in the breach.

**Meaningful Use**

In addition to the HIPAA rule changes, HITECH introduced programs and funds for enhanced privacy and security protections, standards development, and certification infrastructure for EHRs. The Centers for Medicare and Medicaid Services (CMS) was charged with providing guidance and defining requirements for professionals and hospitals that adopt EHR technology. CMS established an incentive program with categories, objectives, and measures for EHR technology. The requirements to receive funds are defined in three stages. Privacy and security is a core set for stage 1 and 2. Stage 3 will be defined in 2016.

<table>
<thead>
<tr>
<th>Objective</th>
<th>Stage 1</th>
<th>Stage 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objectives</td>
<td>Protect electronic health information created or maintained by the certified EHR Technology through the implementation of appropriate technical capabilities.</td>
<td>Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.</td>
</tr>
<tr>
<td>Measure</td>
<td>Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.</td>
<td>Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308 (a)(1), including addressing the encryption/security of data at rest and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.</td>
</tr>
</tbody>
</table>

---

For more information, see [http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html](http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html)

PCI DSS

An actionable framework for developing a robust payment card data security process to help organizations ensure the safe handling of cardholder information at every step.

The Payment Card Industry Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards including the Data Security Standard. The Council’s five founding global payment brands are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. Each of these companies has agreed to incorporate PCI DSS as the technical requirements for each of their data security compliance programs, meaning any organization of any size that wishes to do business with these organizations (i.e., accept payment cards) must comply with PCI DSS.

PCI DSS provides an actionable framework for developing a robust payment card data security process, including prevention, detection and appropriate reaction to security incidents. The DSS includes twelve requirements for any organization that stores, processes or transmits payment cardholder data. These requirements specify the framework for a secure payments environment.

For purposes of PCI compliance, the essence of the requirements involves three steps: assess, remediate and report.

- **Assess** is taking an inventory of IT assets and processes for payment card processing and analyzing them for vulnerabilities that could expose cardholder data.
- **Remediate** is the process of fixing those vulnerabilities.
- **Report** entails compiling records required by PCI DSS to validate remediation and submitting compliance reports to the acquiring bank and global payment brands you do business with.

Carrying out these three steps is an ongoing process for continuous compliance with PCI DSS requirements. These steps also enable vigilant assurance of payment card data safety.

Each member organization of PCI defines different classifications of merchants requiring a different level of assessment and reporting based on the classification. Generally speaking, large merchants processing multiple millions of transactions for a particular merchant annually will be classified as level 1, meaning the organization must conduct a third party assessment and report annually. Merchants which fall in levels 2 through 4 generally process low millions to thousands of records annually and typically are only required to conduct a self-assessment. A quarterly network scan is required in almost all instances.

PCI provides and maintains a Self-Assessment Questionnaire (SAQ) which is a validation tool for merchants and service providers who are not required to do on-site assessments for PCI DSS compliance. There are four SAQs for various situations depending on how the merchant interacts with the payment card and its information.

For those organizations required to conduct on-site assessment, the Council provides programs for two kinds of independent experts: Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV). QSAs have trained personnel and processes to assess and prove compliance with the PCI DSS. ASVs provide commercial software tools to perform vulnerability scans for payment card systems.

**HITRUST Common Security Framework**

Developed in collaboration with healthcare and information security professionals, the Common Security Framework (CSF) is the first IT security framework developed specifically for healthcare information.
The Health Information Trust Alliance (HITRUST) arose from the belief that information security is critical to the broad adoption, utilization and confidence in health information systems, medical technologies, and electronic exchanges of health information. HITRUST is collaborating with healthcare, business, technology, and information security leaders to build this greater level of trust between organizations through the CSF and a program for assessing and reporting information security controls.

The CSF is a framework which normalizes and cross-references the requirements of existing standards and regulations including federal (e.g., HIPAA, HITECH, Meaningful Use), state (e.g., Massachusetts, Nevada), third party and business (e.g., PCI DSS, ISO, JCAHO) requirements. Additionally, HITRUST has been able to add a degree of prescriptiveness in security requirements that has traditionally been lacking, which makes adoption and compliance more consistent and simpler. The CSF is also scalable based on risk and complexity, accounting for different sizes of organizations and the types of systems used, providing the right level of control based on these factors.

In conjunction with the CSF, HITRUST established the CSF Assurance Program whereby organizations can assess and report their risk exposure against a subset of required controls of the CSF. The CSF Assurance Program provides consistency in the currently disparate assessment and reporting processes utilized by healthcare organizations. Through one program and against one set of requirements, organizations can streamline the number of assessments they conduct each year and how they report the results to third parties, while also managing risk.

Since the CSF Assurance Program is based on existing standards and regulations, HITRUST provides organizations with an excellent solution for conducting risk assessments and managing risk as required by the HIPAA Security Rule and Meaningful Use. OCR has, in fact, issued guidance recognizing HITRUST and the CSF as a viable option for conducting a risk analysis under the HIPAA Security Rule.

Complying with the HIPAA and HITECH standards is the first step towards implementing a robust security program that helps avoid data breaches and eliminate threats. The next step is looking at industry standard best practices and solutions.
Improving Security and Meeting Compliance Needs with Trend Micro

Trend Micro solutions can help healthcare organizations both increase their security posture and address many of the security policy requirements of the various regulations such as HIPAA and HITECH by providing multiple layers of protection for endpoints, data centers, the cloud and networks. Trend Micro security solutions monitor, defend, analyze and address security requirements before, during or after an attack.

Trend Micro offers several security solutions for the healthcare industry.

The Complete User Protection solution delivers security protection at multiple layers (endpoint, application, and network) using the broadest range of protection techniques available. The solution secures physical and virtual endpoints using the broadest range of threat and data protection techniques across all devices and applications. The solution uses anti-malware, advanced threat protection, data protection, vulnerability protection, application control, and web filtering to protect desktops and virtualization environments.

The Cloud and Data Center Security solution, with the Deep Security platform, delivers highly efficient agentless and agent-based protection for physical, virtual, and cloud servers. Deployed at the hypervisor level for maximum efficiency, agentless security protects virtual servers and virtual desktop infrastructure (VDI) without the complexity of endpoint deployments in VMware virtualized environments. To integrate easily into an organization’s existing infrastructure, Deep Security is optimized for leading virtualization solutions and cloud service provider architectures including Amazon Web Services, Microsoft Azure, and vCloud Hybrid Services.

The Custom Defense solution, with its Deep Discovery product set, enables organizations to tailor their protection to detect, analyze, adapt, and respond to targeted attacks. Specialized inspection engines and custom sandboxing simulations identify zero-day malware, malicious communications, and attacker activities that are invisible to standard security defenses. Deep analysis, containment, and remediation are powered by relevant threat intelligence and visibility into network-wide security events. In addition, security update exports enable an effective defense against further attacks.

All three solutions are powered by the most advanced threat intelligence network in the world, the Trend Micro Smart Protection Network, which uses big data analytics delivered through the most sophisticated cloud-based global threat intelligence network. The Smart Protection Network is continually monitored and analyzed by a global team of highly trained threat experts.

To make it easier for organizations to manage security, Trend Micro provides central visibility and control across all of these solutions with Control Manager to cut back on administration headaches.

By improving security at the endpoint, server and network layers, healthcare organizations can protect against many security risks situations that tend to occur due to the nature of a healthcare environment:

- Complete User Protection prevents data loss by allowing administrators to understand where ePHI may be present or unsecured.
- Complete User Protection offers encryption at endpoints.
- Custom Defense protects against gaps in security created by multiple medical devices attached to the network.
- Cloud and Data Center Security protects patient portals and data in the cloud or on servers.
• Smart Protection Network monitors, analyzes, defends and protects against malware, known vulnerabilities and popular attacks faster than competitors. By improving security with Trend Micro solutions, healthcare organizations are helping to meet many of the compliance regulations required by healthcare organizations such as HIPAA, HITECH and PCI DSS. A full listing of the regulations addressed by each of the solutions can be found in the matrix “Trend Micro Healthcare Compliance Solutions Matrix - Meeting IT Security and Compliance Needs for Healthcare Organizations with Trend Micro Security Solutions” on the Trend Micro website at www.trendmicro.com.

For more information about Trend Micro individual solutions, please also read the following white papers at www.trendmicro.com:

• Trend Micro ‘Cloud and Data Center Security Solution’ - Meeting IT Security and Compliance Needs for Healthcare Organizations with Trend Micro Security Solutions
• Trend Micro ‘Complete User Protection Solution’ - Meeting IT Security and Compliance Needs for Healthcare Organizations with Trend Micro Security Solutions
• Trend Micro ‘Custom Defense Against Targeted Attacks Solution’ - Meeting IT Security and Compliance Needs for Healthcare Organizations with Trend Micro Security Solutions

---

9 Consumer EPP Comparative Analysis, Socially Engineered Malware, Randy Abrams, Jayendra Pathak, Mohamed Saher, Ahmed Garhy, NSS Labs, 2014