Security and Privacy for Healthcare Providers
Security and Privacy for Healthcare Providers

Contents

Executive summary .................................................. 1
Introduction .......................................................... 2
Breaches happen .................................................... 3
A host of security regulations for healthcare organizations ................... 4
HITECH .............................................................. 4
Security breach notification mandate ................................ 4
Heightened HIPAA enforcement ................................... 4
Medical identify theft .................................................. 5
PCI-DSS ............................................................... 5
State regulations ....................................................... 5
Broad range of challenges ........................................... 6
Best practices for security and privacy for healthcare providers ............ 6
Security and risk assessment ......................................... 6
Data loss prevention ................................................... 6
Endpoint encryption .................................................... 7
Protecting the infrastructure ......................................... 8
Intrusion protection ..................................................... 9
Secure management of systems and devices ................................ 9
Security management .................................................. 9
Automation of compliance .......................................... 10
Conclusion ............................................................ 13
Executive summary
As healthcare providers automate their medical records, clinical systems, and medical imaging, protecting the privacy of patient information and securing IT infrastructures is becoming increasingly challenging. Healthcare organizations are facing more security threats that increase the risks of inappropriate access to patient information, inability to access the information, and impaired integrity of the information. New security and privacy laws for healthcare, heightened enforcement, and stiffer penalties have increased the urgency of addressing security risks.

In this threat landscape, healthcare organizations need to secure protected health information and critical systems as they support operational requirements for providing clinicians with continuous access to information. An effective security management process for a healthcare organization should target specific areas of risk, implement focused security controls for those areas, and automate the monitoring and measurement of controls.

Many healthcare organizations are working with their business partners and security vendors to design and implement security and privacy measures to support their deployments of electronic medical records systems. This white paper describes the challenges of security and privacy in the healthcare environment, and details best practices for assessing risk, preventing loss of healthcare data, meeting regulatory requirements, and securing critical systems with minimal impact on the end user—or on quality of patient care.
Introduction

Increased focus on improving quality of care, reducing costs, attracting referrals, and retaining top talent drives automation and adoption of electronic record systems in the healthcare environment. These trends include increased interconnections, which enable around-the-clock patient information access for physicians as well as new methods of communication between providers, payers, pharmacies, and patients. In addition, they support communication with external service providers such as billing, transcription, and radiology imaging interpretation services.

The expanding scope of interconnected networks between hospitals, clinics, physicians’ offices, remote contractors, suppliers, university networks, and other external parties is changing the footprint and characteristics of the secure enterprise architecture. Laptops and mobile devices are proliferating both inside and outside the hospital—as are interconnected medical devices that, increasingly, operate on common IT platforms and are susceptible to the same security risks as traditional IT devices. For example, physicians look at patient data from handheld devices while moving within the hospital and outside it, Providers’ security perimeters are expanding beyond the internal networks they typically manage to a large number of critical endpoints outside those networks. In this constantly evolving environment, traditional security measures such as firewalls, antivirus, and intrusion detection and prevention systems are no longer providing the required levels of granularity, protection, and enforcement required for compliance with HIPAA and other security and privacy regulations.

A relatively new driver of automation in healthcare—especially in the adoption of electronic medical records—is the American Recovery and Reinvestment Act (ARRA) of 2009. ARRA includes $19 billion in direct funding for healthcare IT and the promotion of electronic medical records. In order to receive financial incentives, healthcare providers will need to demonstrate “meaningful use” of electronic record systems. Requirements for meaningful use are expected to include provisions for ensuring privacy and security of patient data, as well as sharing data with health information exchanges (HIEs), which adds another layer of security risk for providers.
Breaches happen
Increasing automation in the healthcare environment and broader access to patient information are expanding the risk of data breaches. Avoiding these data breaches without disrupting workflow or limiting rapid access for authorized users can be challenging. Unfortunately, data breaches are not rare events. According to the Privacy Rights Clearinghouse, more than 260 million “records” of all types have been breached in the U.S. since January 2005.¹

And data breaches are costly. According to the results of a PGP-sponsored 2008 Ponemon Institute survey of 43 organizations, the total average cost of a data breach increased to more than $200 per record compromised, and the average total cost per reporting company was more than $6.7 million per breach. Almost 90 percent of all cases involved insider negligence, according to the study. Ponemon also found that the average cost of a healthcare breach ($282) is higher than the average across all industries.²

Recent examples highlight the potential severe impacts of data breaches in the healthcare industry. In May 2009, California regulators fined Kaiser Permanente $250,000—the maximum penalty allowable—for failing to prevent healthcare workers from accessing the electronic health records of a woman who had given birth to octuplets. This penalty, assessed under a new California law, shows the potential seriousness of enforcement in high-profile and celebrity health record-leak cases.³

Another recent breach shows that healthcare professionals themselves—not just organizations—may be held accountable. A medical director, an account representative, and an emergency room coordinator at the St. Vincent Infirmary Medical Center in Little Rock, Arkansas, pled guilty to violations of HIPAA health information privacy provisions. Each admitted to accessing a patient’s records without a legitimate purpose. As a result of these convictions, each of the three faces a maximum penalty of a $50,000 fine, one year in prison, or both.⁴

In a third example that shows the pervasiveness of inadvertent or negligent release of protected health information (PHI) by insiders, not hackers, a company that transcribes physician dictation posted records of more than 1000 patient visits to Northeast Orthopedics (Albany, New York) on the Internet. This violation of patient privacy laws could result in fines of up to $25,000.⁵

In addition to the potential costs of data breaches, healthcare providers face potential adverse impact upon their reputations when they must disclose a data breach. Publicity about a breach in local and national media may cause providers to lose patients (as well as clinicians and physicians) due to reputation damage stemming from the security breach.
A host of security regulations for healthcare organizations

A broad range of security and privacy-related regulations apply to healthcare providers—including new or expanded provisions in the Health Information Technology for Economic and Clinical Health (HITECH) Act portion of the American Recovery and Reinvestment Act (ARRA)—heightened enforcement of HIPAA, the Federal Trade Commission (FTC) “Red Flags” identity theft prevention rules, the Payment Card Industry Data Security Standards (PCI-DSS), and state regulations.

HITECH

To improve the adoption of electronic medical record systems, the HITECH Act toughens HIPAA security and privacy regulations, increases fines and enforcement, expands applicability, and creates the first national data breach notification law.

Some penalties have already been levied. Federal regulators reached a resolution agreement with Seattle-based Providence Health & Services to pay $100,000 for HIPAA privacy and security rules violations stemming from the system's loss of electronic backup media and laptop computers with protected health information. CVS Pharmacy agreed to pay $2.25 million to settle allegations of HIPAA violations.

Security breach notification mandate

The HITECH data breach notification law is a significant change with major impact. If a breach of an organization’s “unsecured” protected health information occurs, the organization must within 60 days notify all individuals whose data was breached. If information in a breach is “undecipherable—in other words, if it is encrypted—then notification is typically not required. However, a hospital may not be able to encrypt everything or know conclusively which of its breached data was encrypted. Identifying all the locations where protected health information (PHI) resides and then determining where encryption is needed are major challenges that can be overcome by conducting a thorough assessment before implementing an encryption technology.

Heightened HIPAA enforcement

Enforcement of healthcare data privacy provisions is becoming more aggressive, and fines will continue to increase. The HITECH Act gives state attorneys general authority to bring civil suits in Federal District Court against individuals who allegedly violate HIPAA. The HITECH penalties for unknowingly violating HIPAA are $100 to $25,000 per violation. For violation due to “reasonable cause,” the penalty is $1000 to $100,000 per violation. In case of “willful neglect,” the minimum penalty is $10,000 and the maximum is $250,000. For willful neglect that is not corrected within 30 days, the minimum penalty is $50,000 and the maximum is $1,500,000.

Medical identity theft
Hospitals are increasingly a target for the underground economy, including those criminals who engage in the growing problem of medical identity theft. This involves criminal use of a victim’s Social Security number, insurance information, or health records to obtain medical goods or services or to submit false medical claims. This threat poses multiple problems for victims—damage to both their medical records and their financial wellbeing, exacerbated by the complexity of procedures required to correct the medical records. New Federal Trade Commission (FTC) rules are designed to protect against identity theft. These “Red Flags” rules require that all businesses—including hospitals, physicians’ offices, and other healthcare providers—implement programs to detect and report signs of identity theft, such as suspicious documents, activity, or conflicts in identifying information.9

PCI-DSS
Because many healthcare providers accept credit cards, they are also required to comply with the Payment Card Industry Data Security Standards (PCI-DSS), which are imposed by a nongovernmental organization. Healthcare providers are typically well informed about state and federal data privacy protection laws, but many are not aware of the PCI-DSS requirements to implement security controls for credit card processing. The risk of a data breach in this area increases as more patients pay healthcare fees and copayments using credit cards or flexible spending account debit cards. At the state level, Minnesota’s Plastic Card Security Act imposes liability for losses or damages resulting from a breach of credit card data.10

State regulations
In September 2008, Massachusetts issued a set of regulations, referred to as “201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth.” Originally intended to take effect January 31, 2009 but now extended to January 1, 2010, MA 201 CMR 17 may be the most wide-ranging state data privacy regulation in protecting personal information. It defines minimum data protection standards for safeguarding personal information in both paper and electronic records. The regulation applies to any organization (including healthcare providers) that owns, licenses, stores, or maintains personal information about a Massachusetts state resident—indepenedent of whether they have a physical presence (e.g., office or employees) or whether the services were provided in Massachusetts.

California’s healthcare data privacy laws (Assembly Bill 211 and Senate Bill 541) impose penalties on individuals and institutions that fail to protect the privacy of patient medical records. These laws impose fines, misdemeanors, potential for civil action, and further investigation by a new enforcement agency called the Office of Health Information Integrity.

**Broad range of challenges**
Healthcare providers face many challenges in complying with these complex regulations. They need to support increased interconnections and automation in their healthcare environments, implement security measures without disrupting the workflow of authorized users, and avoid data breach costs and damage to their reputation.

Limited IT budgets also impose constraints in many healthcare organizations. The complexity of ensuring compliance with security- and privacy-related regulations in healthcare and ensuring what policies and standards should be implemented requires solutions that explicitly address these challenges and can be integrated into an organization’s existing infrastructure and business processes.

**Best practices for security and privacy for healthcare providers**
Best practices for security and privacy in the healthcare industry require an end-to-end risk management process:

- **Assessment.** The process typically begins with a thorough security and risk assessment along with determination of the healthcare organization’s level of acceptable risk.
- **Controls.** The second step is to determine what mitigating controls will be implemented to reduce the identified risk to an acceptable level. This often requires additional security controls in the healthcare organization.
- **Compliance.** The next step is to monitor, measure, and report compliance with security and privacy requirements.

**Security and risk assessment**
In today’s environment, healthcare organizations need to balance the operational needs for availability of patient information with the need to protect that information from unauthorized disclosure. The Symantec Information Exposure Assessment provides healthcare organizations with a holistic and data-centric view of their information risk. By combining security consulting services and data prevention loss technologies, Symantec provides healthcare organizations with not only a detailed analysis of their exposure to internal and external data breaches, but also a qualitative assessment of actual data loss risk across networks, Web applications, storage, and endpoints. The program identifies locations where protected health information is wrongfully exposed and discovers vulnerabilities in existing security solutions, as well as comparing the healthcare provider’s existing infrastructure and environment with established security best practices.

After an assessment, Symantec consultants can design a program that offers an optimum level of protection, meeting the healthcare provider’s business needs, budget, and risk tolerance. Once a design is agreed upon, Symantec works closely with the healthcare IT team to efficiently implement a Symantec Threat and Vulnerability Management Program framework. Symantec consultants can train the healthcare IT staff to manage the program or provide continuous onsite management with a Symantec resident consultant.

**Data loss prevention**
Security controls for healthcare environments should focus on protecting patient and other confidential information, in addition to protecting the various layers of the infrastructure. Content-aware data loss prevention enables hospitals,
health maintenance organizations, and healthcare services companies to monitor and protect confidential data contained in patient medical histories or diagnostic results, as well as billing and insurance information. This information-centric solution also provides the visibility and control required to demonstrate compliance with HIPAA requirements for electronic transactions and data security.

Symantec™ Data Loss Prevention reduces risk of confidential data loss via a unified data loss prevention solution to discover, monitor, protect, and manage protected health information wherever it is stored or used (see figure 1).

Data Loss Prevention has enabled leading healthcare companies to:

- Secure patients’ private medical histories
- Demonstrate compliance with regulations such as HIPAA, PCI, and state data privacy laws
- Enable secure communications between doctors, pharmacies, and insurance companies
- Protect employee and network physicians’ personal information

**Figure 1. Symantec Data Loss Prevention is a solution for discovering, monitoring, protecting, and managing confidential data**

**Endpoint encryption**

As data travels across various environments and is stored on an ever-growing array of endpoint and storage devices—including PCs, laptops, and removable devices—the need for strong encryption is becoming evident. If data received or accessed by unauthorized personnel (such as data on a lost USB drive or stolen laptop, or an email message sent to a wrong person) is encrypted (“undecipherable”), then it is typically not considered a breach under the HITECH Act and similar state laws. Yet healthcare facilities need to determine the extent of encryption they should adopt. For example, a hospital could decide to encrypt data only where there is the greatest risk of loss (such as patient data in email messages and on USB drives), and not in internal databases or systems where access is controlled—and where workflow and performance impact must be minimized.
Symantec™ Endpoint Encryption offers a security solution for healthcare organizations that protects endpoints with encryption and prevents unauthorized access. Endpoint Encryption protects information and prevents accidental data loss, safeguards desktops and laptops against unauthorized access, and provides encryption of data on hard disks to meet government directives and regulations.

**Protecting the infrastructure**
Protecting endpoint devices—including laptops, desktops, mobile devices, servers, and even medical devices with embedded operating systems—in the healthcare environment against increasingly sophisticated malware attacks is another critical area for healthcare IT professionals. Many new, sophisticated threats can evade traditional security solutions, leaving healthcare organizations vulnerable to data theft and manipulation, disruption of critical services, and damage to brand and reputation. To stay ahead of this emerging breed of stealthy and resilient security threats, providers need proactive endpoint protection.

Symantec™ Endpoint Protection integrates antivirus, antispyware, firewall, intrusion prevention, and device and application control in a single package (see figure 2). In addition to signature-based protection, Endpoint Protection provides threat prevention that protects endpoints from attacks that have not previously been seen. It includes technologies that automatically analyze application behaviors and network communications to detect and block suspicious activities, as well as administrative control features that allow healthcare IT administrators to deny specific device and application activities deemed as high risk. Healthcare IT administrators can even block specific actions based on the location of the user.

![Figure 2. Symantec takes a unified approach to endpoint protection](image-url)
This multilayered approach lowers risk and provides assurance that healthcare provider assets are protected. Whether attacks on those assets come from malicious insiders or are external in origin, endpoints will be protected.

**Intrusion protection**

While content-aware data loss prevention focuses on protection of information itself, intrusion protection addresses the healthcare organization’s network. Intrusion protection involves detecting abnormal activities on the network; curtailing those activities based on pre-established policies; and centrally managing the configuration, deployment, monitoring, and reporting of security policies and network activities.

Symantec™ Critical System Protection provides prevention techniques that shield operating systems, applications, and services by defining acceptable behaviors for each function. The solution then protects systems from misuse by unauthorized users and applications through system and device controls that lock down configuration settings, file systems, and the use of removable media. To help ensure host integrity, system protection and regulatory compliance, Critical System Protection provides monitoring, notification, and auditing features. The solution enables cross-platform server auditing and compliance enforcement.

**Secure management of systems and devices**

Hospital technology is evolving quickly. In an effort to meet their strategic business objectives, organizations regularly add new desktops, laptops, mobile devices, and specialized patient care systems. This rapid pace of change has resulted in hospitals having to maintain numerous isolated IT assets. Device tracking is complicated and cumbersome. Hospital systems and devices that are not centrally managed are more subject to security vulnerabilities—because of configuration problems or missing software patches, for example.

Altiris™ Client Management Suite from Symantec is a centralized management solution that enables hospitals to deploy software and patches to individual devices with minimal downtime and disruption to hospital operations. The ability to manage clients remotely and automatically enables IT departments to perform maintenance tasks transparently in the background, minimizing interruptions to service and clinical staff, and also improving the security posture of a well-managed network.

**Security management**

Healthcare providers face an escalating global threat landscape, new compliance rules and regulations, and constrained security budgets. Combined, these challenges place high demands on organizations whose job it is to secure the healthcare enterprise. To stay ahead of today’s threats with limited staff resources, organizations benefit from partnering with security experts who deliver proactive protection for their networks with 24x7 monitoring.

Symantec™ Managed Security Services puts aspects of security operations under the management of experienced specialists, offering healthcare organizations a higher level of protection for their mission-critical information assets. A complete service portfolio is available to help demonstrate healthcare IT compliance, minimize the impact of security events, and mitigate security risks at an acceptable cost. In the face of today’s emerging threats, Symantec delivers real-time threat monitoring and analysis to minimize any impact on business operations and reduce overall security risk.
Automation of compliance

Today, the complexity of ensuring compliance and strong IT governance in a healthcare organization is increased by the variety of security issues that must be monitored and the need to comply with multiple external mandates, including HIPAA, state privacy laws, and the PCI-DSS standards for processing credit card payments. Recent research indicates that companies investing in point products for each compliance mandate they face will spend significantly more on IT compliance than those that implement a solution suite to manage multiple mandates. Healthcare organizations also need to keep up with changes in these industry regulations, updating their policies and control statements accordingly.

Most organizations currently handle IT risk and compliance challenges through costly, time-consuming manual processes. They use a combination of spreadsheets, checklists, and manually distributed questionnaires to define and manage policies and assess effectiveness of technical and procedural controls with respect to these policies. These manual processes are neither scalable nor easily repeatable. They can also be error-prone. Other organizations use point-product solutions to help with different stages in the compliance life-cycle – for example, one solution to assist with data collection and another to assist with policy management and reporting. This approach leads to higher costs due to integration, ongoing support for each solution, and redundant efforts to evaluate the same controls across multiple regulations.

Symantec™ Control Compliance Suite helps healthcare organizations prepare for compliance audits by offering a holistic approach to IT risk and compliance. The solution allows organizations to:

- Define policies for multiple industry regulations (HIPAA, PCI-DSS, state laws) and best practice frameworks
- Automatically map policies to control statements
- Automatically assess the effectiveness of both technical and procedural controls
- Generate dashboard reports as auditable evidence of compliance posture
- Prioritize remediation efforts based on risk

Figure 3. Symantec Control Compliance Suite provides end-to-end coverage for the healthcare IT compliance lifecycle
A complementary product, Symantec™ Security Information Manager is a real-time security incident tracking tool. It enables healthcare organizations to collect, store, and analyze log data, as well as monitor and respond to security events to meet IT risk and compliance requirements. It can collect and normalize a broad scope of event data and correlate the impact of incidents based on the criticality to business operations or level of compliance to various mandates. The solution prioritizes incidents using its built-in asset management function, which is populated using scanning tools and allows confidentiality, integrity, and response ratings and policies to be assigned to help prioritize incidents.
### Key challenges and corresponding Symantec solutions

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Symantec solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Analyze exposure to internal and external data breaches</td>
<td>Symantec Threat and Vulnerability Management Program</td>
</tr>
<tr>
<td>• Assess risk of information loss across networks, Web applications,</td>
<td>Symantec Information Exposure Assessment</td>
</tr>
<tr>
<td>storage, and endpoints</td>
<td></td>
</tr>
<tr>
<td>• Design an information protection program</td>
<td></td>
</tr>
<tr>
<td>• Discover, monitor, and protect confidential information</td>
<td>Symantec Data Loss Prevention</td>
</tr>
<tr>
<td>• Demonstrate compliance with HIPAA, PCI, and state privacy laws</td>
<td></td>
</tr>
<tr>
<td>• Encrypt data on desktops, laptops, and disks</td>
<td>Symantec Endpoint Encryption</td>
</tr>
<tr>
<td>• Protect endpoints from malware and threats (antivirus, antimalware,</td>
<td>Symantec Endpoint Protection</td>
</tr>
<tr>
<td>firewall, intrusion prevention, and device and</td>
<td></td>
</tr>
<tr>
<td>application control)</td>
<td></td>
</tr>
<tr>
<td>• Protect systems from misuse by unauthorized users and</td>
<td>Symantec Critical System Protection</td>
</tr>
<tr>
<td>applications</td>
<td></td>
</tr>
<tr>
<td>• Lock down configuration settings and file systems, and control the use</td>
<td></td>
</tr>
<tr>
<td>of removable media</td>
<td></td>
</tr>
<tr>
<td>• Prepare for compliance audits</td>
<td>Symantec Control Compliance Suite</td>
</tr>
<tr>
<td>• Automate policy management and checking of technical and procedural</td>
<td>Symantec Security Information Manager</td>
</tr>
<tr>
<td>controls</td>
<td></td>
</tr>
<tr>
<td>• Track and monitor security incidents</td>
<td></td>
</tr>
<tr>
<td>• Manage systems, devices, and configurations</td>
<td>Altiris Client Management Suite from Symantec</td>
</tr>
<tr>
<td>• Deploy software and patches</td>
<td>Altiris™ Server Management Suite from Symantec</td>
</tr>
<tr>
<td>• Track assets and manage licenses</td>
<td>Altiris™ Service and Asset Management Suite from Symantec</td>
</tr>
<tr>
<td>• Manage IT risk and maximize IT performance with experienced</td>
<td>Symantec Security Consulting Services</td>
</tr>
<tr>
<td>specialists</td>
<td>Symantec Managed Security Services</td>
</tr>
</tbody>
</table>
Conclusion
Symantec advocates an end-to-end risk management approach to help ensure security and privacy in the healthcare industry. This approach identifies risks as it finds efficiencies. It leverages existing infrastructure, and it integrates both existing and future products into a solution that automates security and compliance functionality. Finally, it focuses on a risk management process that encompasses assessment of information exposure and vulnerabilities, implementation of security controls, and automation of compliance.

With leading risk management expertise in areas ranging from vulnerability assessment and data loss prevention to endpoint encryption and protection, compliance automation, and more, Symantec is able to provide a comprehensive security and privacy solution for healthcare providers.
About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com