



Confidence in a connected world.

## **Automating IT Regulatory Compliance for Healthcare Providers**



# Automating IT Regulatory Compliance for Healthcare Providers

## Contents

Executive summary . . . . .	4
<b>Regulatory compliance for healthcare: A changing landscape . . . . .</b>	<b>4</b>
Challenges of compliance . . . . .	6
Benefits of adopting an automated approach to compliance . . . . .	8
<b>Compliance best practices for healthcare providers . . . . .</b>	<b>9</b>
Defining the compliance effort . . . . .	10
Controlling and managing the compliance effort . . . . .	10
Governing the compliance response . . . . .	11
<b>Symantec’s portfolio of regulatory compliance solutions for healthcare providers . . . . .</b>	<b>12</b>
<b>Conclusions . . . . .</b>	<b>12</b>

## **Executive summary**

This paper is one of a series outlining the challenges healthcare providers face in information technology (IT), and the best practices for meeting those challenges. This paper focuses on the specific topic of regulatory compliance.

Healthcare providers face a constantly changing regulatory landscape. Faced with numerous mandates to satisfy, they also grapple with an ever-increasing body of electronic data that they must protect and secure. While acknowledging the challenges implicit in implementing IT security, healthcare providers are also recognizing that automating their compliance efforts can bring benefits as well as shield their institutions from the potentially disastrous consequences of noncompliance. Benefits include freeing up IT personnel to focus on activities that directly improve facility operations or enhance the quality of patient care. Just as important, failure to comply can negatively impact a provider's bottom line, reducing revenues as a result of loss of accreditation, exposing the provider to potential monetary penalties or litigation costs, and even causing a provider to close its doors.

Best practices suggest implementing a more measured, holistic approach that establishes a foundation for ongoing compliance, and automating the process with appropriate technological tools. Arming the right personnel with this combination offers the best roadmap for navigating today's regulatory landscape.

## **Regulatory compliance for healthcare: A changing landscape**

Today, healthcare providers must thrive in a landscape of constantly changing regulations imposed by a dizzying variety of organizations: federal, state, and even local governments, accrediting bodies, and regional health organizations. The Health Insurance Portability and Accountability Act (HIPAA) security and privacy provisions and the standards promulgated by the Joint Commission on Accreditation of Healthcare Organizations (Joint Commission, formerly known as JCAHO) represent the most significant standards healthcare providers face. HIPAA requirements impose a federal mandate, while compliance with the Joint Commission standards is voluntary. However, since the Joint Commission accredits nearly 17,000 healthcare organizations nationwide and Joint Commission accreditation is critical for Medicare and Medicaid reimbursement eligibility, compliance with its standards is even more important. Any loss of accreditation can jeopardize this reimbursement, which represents a significant portion of many providers' revenues, and also impacts a hospital's reputation and ability to attract patients and staff.

## Automating IT Regulatory Compliance for Healthcare Providers

The Joint Commission standards for information management parallel the HIPAA privacy and security provisions; the latter establish regulations for the use and disclosure of Protected Health Information (PHI), which is broadly interpreted as any part of a patient's medical record or payment history (e.g., information about health status, provision of healthcare, or payment for healthcare). Complementary to the HIPAA privacy rule, the security rule deals specifically with Electronic Protected Health Information (EPHI), identifying three types of security safeguards required for compliance (administrative, physical, and technical) as well as various standards for each type and required and addressable implementation specifications. Other critical provisions require implementation of audit controls, retention of audit logs for seven years, and the observation of a standard of due care with respect to security monitoring of critical data (a standard that essentially requires real-time monitoring).

A recent audit of HIPAA security compliance undertaken by the U.S. Department of Health and Human Services (HHS) at Piedmont Hospital in Atlanta in March 2007 has many industry members paying more serious attention to HIPAA requirements and their own institution's compliance activities.<sup>1</sup> Noncompliance with HIPAA provisions carries significant risks, including civil and criminal penalties.

Joint Commission standards and HIPAA requirements are not the only regulatory challenge for healthcare providers. For instance, healthcare providers must also comply with Payment Card Industry Data Security Standards (PCI DSS), since providers accept credit cards for payments. Sarbanes-Oxley regulations pose compliance challenges for some providers who voluntarily comply with these standards. What's more, many regional organizations face a patchwork of regulations that change from one jurisdiction to another.

Healthcare providers continue to grapple with the best ways to implement IT-based compliance programs. According to the annual Global State of Information Security Survey 2007, while fully one-half of all healthcare providers link security to privacy or regulatory compliance;<sup>2</sup> many still do not conduct the most basic of activities to ensure compliance. For instance, 65 percent of healthcare providers do not conduct annual or semiannual risk assessments, while 61 percent do not audit or monitor user compliance; nearly as many (58 percent) have not measured or reviewed the effectiveness of their security policies and procedures in the past 12 months.<sup>3</sup> These statistics point to the real challenges behind regulatory compliance, which continue to increase with the evolution in the healthcare industry toward greater use of electronic records of all types.

<sup>1</sup> "HIPAA Audit at Hospital Riles Health Care IT," Jaikumar Vijayan, Computerworld, June 15, 2007. [www.computerworld.com](http://www.computerworld.com)

<sup>2</sup> "Information Security Still An Issue In Health Care," Vance Cariaga, Investor's Business Daily, September 7, 2007. [www.investors.com](http://www.investors.com)

<sup>3</sup> Ibid.

### **Challenges of compliance**

The real challenges in compliance lie not just with specific provisions that change from one month or year to the next, but rather with the underlying business issues healthcare providers face:

- The complexity of the compliance task
- The costs of the compliance effort
- The potential costs of noncompliance

### ***Complexity***

Compliance requirements at a variety of jurisdictional levels often result in the necessity for numerous ongoing, simultaneous compliance efforts. Additional factors that increase complexity include lack of automation; inconsistency of processes across departments; multiple ways of testing, measuring, and reporting on the same IT control process; and multiple IT infrastructures that are often cobbled together as a result of mergers or acquisitions.

The lack of automation is a major stumbling block for many providers. For instance, Touchstone Behavioral Health estimates that prior to automating its compliance program, it spent up to two person-weeks gathering log files and the resultant sets of policies. Based in Glendale, Arizona, with four locations in Phoenix as well as locations in Flagstaff and Tucson, the organization provides behavioral treatment programs for at-risk children. With 200 employees, a high percentage of laptops in use in the field, and only four IT staff, Touchstone found compliance efforts burdensome.

The lack of automation embraces the human resource dimension. Institutions may ponder who should manage compliance in their organizations, as well as how many people are needed to ensure adequate performance of compliance efforts. Ancillary issues include the ongoing need for specialized training and monitoring of employee satisfaction (e.g., repetitive manual tasks forced upon IT personnel increases turnover).

Another characteristic of this complexity is the visibility of the data itself. Because of overlapping compliance efforts and duplicative IT infrastructures, many healthcare providers struggle to generate reports that provide a clear snapshot of data flows, specify who has access to which files and databases, and determine when specific data have been transmitted and by whom. Instead, many providers choose to hire specialized data retrieval services or spend exorbitant numbers of person-hours assembling the data internally.

### ***Cost and impact on productivity***

Perhaps even more critical in a time when budgets are lean is the cost issue. Many healthcare providers currently conduct their compliance programs manually, at a cost of hundreds, if not thousands of person-hours annually—resources that could go into patient care functions if the compliance program were automated. Kettering Medical Center Network's experience offers an example. Prior to automating its compliance efforts, the institution estimates it spent three or four days each time it needed to validate a specific set of security policies on the institution's 200 servers; following automation, this was slashed to half a day.<sup>4</sup> In fact, some solution providers estimate that IT staff time can be halved with successful implementations of automated compliance tools.

### ***Potential costs of noncompliance***

The costs of noncompliance also pose a risk. Loss of Joint Commission accreditation can jeopardize Medicare/Medicaid reimbursements, as well as loss of general revenues if doctors and patients select alternative facilities. HIPAA violations can result in civil and criminal penalties, including monetary penalties of \$100 per violation with a maximum of \$25,000 per year, per violation.<sup>5</sup>

In addition to these potential regulatory penalties, noncompliance can result in other costs. Increasingly, law enforcement authorities and courts are interpreting standards such as HIPAA in ways that have profound implications for healthcare providers. For instance, in 2006 a North Carolina Court of Appeals ruling allowed a plaintiff to use the HIPAA standard as a "standard of care" for an individual action.<sup>6</sup> In some cases, security breaches that would constitute noncompliance can even contribute to a provider going out of business. Verus Inc., a Bellevue, Washington, IT contractor that built and maintained Web sites and services for dozens of hospitals nationwide, closed its doors in the summer of 2007 after being implicated in security breaches. These breaches, which occurred in at least five different hospitals in the U.S., involved the exposure of patient data when a Verus employee left a firewall down following the transfer of data between servers.<sup>7</sup>

<sup>4</sup> "Kettering Medical Center Network: Facilitating a Healthy and Secure Hospital Network With a Comprehensive Symantec Solution," Symantec success story, 2006.

<sup>5</sup> [www.hipaadvisory.com/Regs/compliancecal.htm](http://www.hipaadvisory.com/Regs/compliancecal.htm). Accessed September 24, 2007.

<sup>6</sup> "HIPAA Audit at Hospital Riles Health Care IT," Jaikumar Vijayan, Computerworld, June 15, 2007. [www.computerworld.com](http://www.computerworld.com).

<sup>7</sup> "Medical IT Contractor Folds After Breaches," Tim Wilson, August 15, 2007. [www.darkreading.com](http://www.darkreading.com).

## Benefits of adopting an automated approach to compliance

Automating compliance programs offers healthcare providers the ability to overcome these challenges and realize a range of benefits. By reducing staff time spent on compliance activities, providers can devote more IT resources to supporting or enabling better patient care. Reductions in staff time are significant; at Baptist Health South Florida, the IT staff was able to reduce security audit preparation time from 12 hours to 15 minutes.

This time savings is often put to good use elsewhere. Since being relieved of many of the demands of compliance management, for instance, the IT team at Kettering has been able to focus on more valuable initiatives, such as a Simple Sign On application that enables 1,500 more hours of direct patient care by clinicians every day.<sup>8</sup> Susan Fronapfel, manager of information technology and security at Danbury Hospital, agrees. "More time for our IT staff means that we can focus on other areas, such as the email system and online billing, to improve hospital operations."<sup>9</sup>

In addition to enabling IT staff to focus on other activities, Danbury Hospital, a regional medical center serving residents of Connecticut and New York, has recognized other benefits. By automating its compliance program, the institution "consolidated the existing rule base of our multiple firewalls and fine tuned the rules for tighter control," notes Brenda Plaag, chief privacy officer. "We now have solid statistical evidence demonstrating the difference between our security coverage before and after."<sup>10</sup> This illustrates the improvement in compliance efforts that automated tools can bring to a well designed compliance program.

2007 research conducted by the IT Policy Compliance Group also suggests a strong relationship between effective compliance programs and a strong security environment (see Table 1). See also Critical Infrastructure Security for Healthcare Providers in this Best Practices Series for a detailed discussion of security issues.

**Table 1. Compliance deficiencies, business disruptions, data losses, and thefts.**

Performance spectrum	Percentage of organizations	Number of IT compliance deficiencies to pass audit	Number of security events resulting in business disruptions	Number of unreported losses or thefts of sensitive data
Lagging firms	20%	26	17	22
Normative firms	67%	6	6	5
Leading firms	13%	2	2	2
Sample		1,779	1,269	694

Data courtesy of IT Policy Compliance Group, 2007.

<sup>8</sup> "Kettering Medical Center Network: Facilitating a Healthy and Secure Hospital Network With a Comprehensive Symantec Solution," Symantec success story, 2006.

<sup>9</sup> "Danbury Hospital Works with Symantec," [www.huliq.com/7830/danbury-hospital-works-with-symantec](http://www.huliq.com/7830/danbury-hospital-works-with-symantec), accessed October 4, 2007.

<sup>10</sup> Ibid.

## Automating IT Regulatory Compliance for Healthcare Providers

Another benefit providers appreciate is the ease of use and convenience offered by compliance tools. Dashboard style screens offer at-a-glance visibility into compliance efforts. “We literally have the ability to take a snapshot of our dashboard at any point in time,” says Touchstone IT Director Steven Porter.<sup>11</sup>

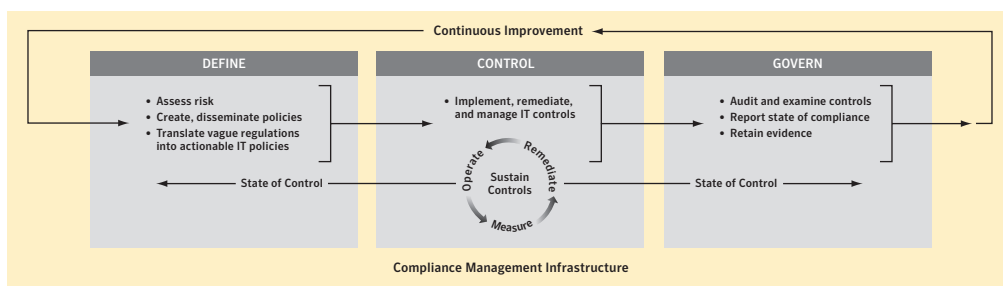
Other providers have realized substantial cost savings. When Kettering automated its compliance program, it realized annual savings of \$18,000 in staff time.<sup>12</sup>

### Compliance best practices for healthcare providers

An initial best practice for implementing a successful compliance program is recognizing at the outset that it involves deployment not only of technological tools capable of automating compliance efforts, but also of appropriate business processes, policies, and personnel. Individual compliance products that address specific regulatory provisions may provide a stopgap benefit, but a holistic and strategic lifecycle approach will ensure a stable, continuous program that enables compliance for the long run.

Such a holistic approach involves three components:

- Defining or identifying the parameters of the compliance program
- Controlling and managing the compliance effort
- Governing the compliance response



**Figure 1. A holistic approach to regulatory compliance involves three phases in an initial implementation, and then an ongoing compliance program that extends beyond merely meeting specific compliance requirements with individual product solutions.**

<sup>11</sup> “Touchstone Behavioral Health: Providing Security for Sensitive Client Information with a Four-Person Staff—and Help from Symantec,” Symantec Success Story, 2007.

<sup>12</sup> “Kettering Medical Center Network: Facilitating a Healthy and Secure Hospital Network With a Comprehensive Symantec Solution,” Symantec success story, 2006.

### **Defining the compliance effort**

In the first stage, the provider identifies the regulations requiring compliance, and defines its risk categories and the policies it must implement. For instance, HIPAA requires that covered entities conduct a vulnerability assessment; simply performing the activities in this first stage—identifying the required compliance activities as well as the risk categories and needed policies—will satisfy this HIPAA provision. However, many healthcare providers lack the internal resources necessary to conduct such a comprehensive assessment. Similarly, developing specific, actionable policies can be difficult.

That's where teaming with a trusted advisor who brings substantial experience in compliance issues and a comprehensive perspective on information security can reap dividends. The advisor team can immerse itself in the provider's operations and provide hands-on expertise, guiding the assessment as well as assisting with the development of effective policies—and the technology tools necessary to implement those policies effectively.

To complete the objectives at this stage, the compliance team will deploy carefully chosen technology tools that facilitate more comprehensive assessments, such as software that tracks all IT assets as well as software usage and licensing. In parallel, the vulnerability assessment (sometimes referred to as a *risk assessment* or *gap analysis*) will identify the most significant areas of noncompliance. Armed with this information, the compliance team can then create the detailed “to-do” lists necessary to close the identified gaps and achieve compliance. Complementary ongoing efforts include developing appropriate security and privacy business policies.

### **Controlling and managing the compliance effort**

The second component involves controlling and managing the compliance effort. This includes arming managers with the necessary technological tools alongside defined policies that enable them to manage compliance activities effectively. Leading technology solutions include applications that automate compliance by mapping provider policies to multiple frameworks, standards, and regulations. For instance, a network of hospitals in California would need to map its policies to HIPAA, California requirements such as SB1386, and the relevant provisions of the Joint Commission Accreditation Manual, as well as other accrediting organizations.

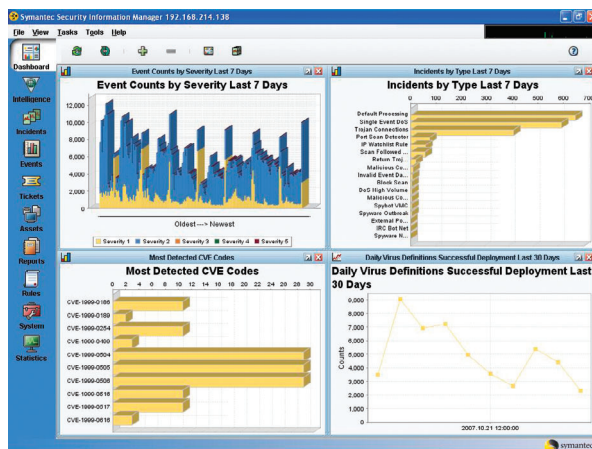
## Automating IT Regulatory Compliance for Healthcare Providers

Another set of technology tools many providers should utilize is data loss prevention systems to prevent the inadvertent transmission of private data to unauthorized third parties. HIPAA Security Rule Administrative Standards and Implementation Specifications (§164.308) address the implementation of policies and procedures to prevent, detect, contain, and correct security violations. The type of violation this refers to might include a situation in which a newly terminated hospital employee accesses patient data with the intent to use or destroy it. Deploying technology tools that monitor providers' networks in real time and identify unauthorized intrusions will satisfy this requirement. For more detailed best practices on electronic medical record (EMR) security, refer to the white paper *"Critical Infrastructure Security for Healthcare Providers"* in this Best Practices series.

### Governing the compliance response

The third and final component of a holistic compliance program refers to the provider's ability to self-audit its compliance activities, generate enterprisewide metrics on its efforts, and report to the appropriate external regulatory bodies.

The latest generation of tools includes dashboard style screens (see Figure 2) that provide at-a-glance information to C-level information security personnel while still being capable of generating the detailed reports required by regulators. Furthermore, compliance reporting can be automated to occur on a scheduled or on-demand basis.



**Figure 2. Compliance solution dashboards offer at-a-glance information about the state of an institution's ongoing compliance activities.**

**Symantec’s portfolio of regulatory compliance solutions for healthcare providers**

Compliance lifecycle stage	Technology tool/need	Symantec product or service
Define	<ul style="list-style-type: none"> <li>Track IT assets, software usage, licensing</li> <li>Identify rogue technologies</li> <li>Conduct risk assessment</li> </ul>	<ul style="list-style-type: none"> <li>Symantec™ Discovery</li> <li>Professional Services/Systems Continuity Service</li> </ul>
Control	<ul style="list-style-type: none"> <li>Map provider policies to frameworks, standards, and regulations</li> <li>Translate vague regulations into actionable policies</li> </ul>	<ul style="list-style-type: none"> <li>Symantec Control Compliance Suite</li> <li>Professional Services/Systems Continuity Service</li> </ul>
Govern	<ul style="list-style-type: none"> <li>Establish baseline configurations</li> <li>Identify exceptions to standards</li> <li>Discover, store, monitor, and report on compliance activities</li> <li>Incident response management</li> </ul>	<ul style="list-style-type: none"> <li>Symantec Control Compliance Suite</li> <li>Symantec Security Information Manager</li> </ul>

**Conclusion**

Healthcare providers can best control their own destiny amidst the ever-changing regulatory landscape by developing and deploying a comprehensive compliance program. Best practices suggest that this program move beyond deployment of piecemeal technology solutions, designed to comply only with the regulation du jour, to embrace a lifecycle approach that integrates technology tools with policies. Such an approach includes:

- Defining or identifying the parameters of the compliance program, including regulations requiring compliance, provider’s risk categories and policies it must implement.
- Automating compliance by mapping policies to multiple frameworks, standards, and regulations.
- Self-auditing, automatic generation of enterprise-wide metrics, and comprehensive reporting to appropriate authorities.

By automating compliance activities, providers can reduce the cost of compliance by eliminating duplication of effort and unnecessary personnel-hours, prevent noncompliance penalties or potential loss of revenue, and avoid costly outsourced auditing services. In addition, healthcare providers can strengthen their relationships with patients and payers by demonstrating a strong commitment to ensuring the security and privacy of personal health information.







## About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world.

The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries.

More information is available at [www.symantec.com](http://www.symantec.com).

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation  
World Headquarters  
20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
+1 (408) 517 8000  
1 (800) 721 3934  
[www.symantec.com](http://www.symantec.com)

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. Printed in the U.S.A.  
11/07 13518081