7 STEPS TO SECURING HEALTHCARE INFRASTRUCTURES USING A CLOUD SECURITY PLAN

With 80 percent of respondents to the inaugural 2014 HIMSS Analytics Cloud Survey reporting that they currently use cloud-based IT services – and others making plans to move their data and mission-critical applications to the cloud in the near future – the industry's digital transformation is well underway.

Today's leading healthcare organizations recognize security as an evolving challenge requiring constant attention and not a one-time check-box item to be crossed-off a to-do list. They understand that compromises to security should not be discovered when a problem, such as a virus, surfaces and responses are not only reactive but oftentimes too late to prevent damages. They also realize that the higher stakes accompanying the industry's transformation mean they can no longer afford to go it alone. Lacking the resources to keep up with the evolution of threats and what it takes to remain secure, many healthcare organizations are leveraging external partnerships to ensure their security plans remain up to the task at hand.

One of the most effective ways to develop cloud security policies is to solicit cross-departmental input.

For healthcare, the top three reasons for adopting cloud services include lower maintenance costs, speed of deployment and lack of internal staffing resources, according to the HIMSS survey. Cloud computing provides compelling cost and strategic benefits, including scalability with reduced capital expenditures and more efficient use of IT resources.

Driven by the need to meet government compliance requirements such as HIPAA, the industry-wide implementation of electronic medical records and the overarching need to reduce healthcare costs, the leap to cloud computing in many ways supports the industry's goal of being more patient-centered and data-driven.

But while healthcare IT professionals may have grown more comfortable storing data in the cloud, security remains a consideration, according to HIMSS. Choosing a service provider with strong security procedures and services can be a strategic move in the right direction, but healthcare organizations need to maintain an active role in security and risk management in order to more easily manage the flood of patient data accompanying the industry's transformation, and to realize the cost savings that cloud computing promises.

By adhering to the following seven-step plan from NaviSite, Inc., a leading provider of hosting, application management and managed cloud services for enterprises, healthcare organizations can bank on a proven methodology for cost-effectively and securely leveraging cloud services.

Produced in partnership with

HIMSS Media

Step 1: Review business goals

Although hospital settings and physician practices can vary greatly, every cloud security plan should begin with a routine assessment of specific business objectives. Security should enable:

- **Technologies:** Authentication and authorization, managing and monitoring, and reporting and auditing technologies should be used to protect, monitor and report on access to information resources
- **Processes:** Methodologies should be established that spell out processes for everything from provisioning and account establishment through incident management, problem management, change control and acceptable use policies so that processes govern access to information
- **People:** Healthcare organizations require access to the proper skill sets and expertise in order to develop security plans that align with business goals

> An effective cloud-computing risk-management program will reduce overall risk, prioritize the utilization of resources and provide your healthcare organization with a long-term strategy.

One of the most effective ways to develop cloud security policies is to solicit cross-departmental input. Including contributions from senior management, finance, sales, engineering, manufacturing, human resources and other stakeholders will ensure that the final security plan aligns with and supports organizational imperatives.

Step 2: Create security policies, procedures and standards

Having a set of guidelines will ensure that all compliance measures are identified and the entire organization is advancing toward the same objectives.

Department of Health and Human Services audits typically involve looking at existing policies, how they have been implemented and whether they are being followed organization-wide. By completing the first four steps outlined here, it will be easier to create security guidelines that can be consistently enforced.

The easiest way to create security policies, procedures and standards is to embrace best practices. Read everything available and apply industry best practices in order to create policies that align with your specific business goals and allow for the development of realistic procedures that are acceptable to your organization.

For healthcare providers, a good example may be found in the provisioning of HIPAA- and HITECH-compliant services to new and existing patients. In order to do so, the healthcare organization must build security policies that define the restrictions when handling Protected Health Information (PHI), procedures that define the process of acquiring PHI and guidelines that promote the general adoption of best practices.

Healthcare organizations can dramatically reduce the learning curve for developing security policies, procedures and standards by leveraging high-performance cloud computing.

Step 3: Maintain a risk management program

An effective cloud-computing risk-management program will reduce overall risk, prioritize the utilization of resources and provide your healthcare organization with a long-term strategy. But only a well-defined and carefully maintained risk-management program will deliver an aggregated view of the risk that an organization is willing to accept. Most organizations assess the value of the asset and the loss expectancy probability before determining whether a risk is acceptable, or if steps should be taken to reduce the chances of that loss. Careful analysis should be conducted regularly to develop responsible programs and to build in the controls and auditing capabilities needed to lower threats and maintain a reasonable security program that protects assets within budgetary guidelines.

Your cloud-computing risk-management program should be audited, and policies should be defined explicitly stating who may accept risk on behalf of the organization. Having a robust risk-management program in place means you have identified your critical assets and established appropriate levels of protection.

Step 4: Support business goals

A well-developed cloud-computing security plan should include goals with measurable results that provide support for the growth and stability of your healthcare organization. It should include compliance programs, technologies and processes with specific results. In many ways, your security plan will become a natural extension of the first two steps.

Step 5: Go for organization-wide support and alignment

To garner support and acceptance of your cloud-computing security plan, prioritize security policies and ensure that they are not in conflict with other policies from different departments. Involvement and support of the plan throughout the organization is critical to its success.

Although establishing levels of security that meet business goals and comply with regulatory requirements and risk- management policies is critical, it is equally important that they can be centrally managed and conveniently implemented with minimal negative impact to productivity. Balancing ease of deployment and organizational acceptance is a necessary trade-off.

NaviSite has found that the key is to budget enough time into the process to foster an understanding of how a healthcare organization develops its services and delivers them to patients and/or affiliated partners. Rather than devoting the bulk of your time to writing policies, plan on spending the majority of your time learning how the organization truly functions, so security can better contribute to its success and not be viewed as a daily battle.

> Rather than devoting the bulk of your time to writing policies, plan on spending the majority of your time learning how the organization truly functions, so security can better contribute to its success and not be viewed as a daily battle.

Step 6: Plan for regular audits and reviews

Regularly reviewing your security plan, reporting on goal progress and auditing the organization's compliance with security policies and procedures are important components of the plan's success. If it is part of your overall business plan, a third-party audit can deliver an impartial review of the controls and report on compliance to established programs. Fully grasping the auditing requirements for your healthcare organization – as well as the frequency of audits – ensures both compliance with relevant requirements and maintenance of best practices for securing enterprise resources.

Step 7: Improve your improvements

The continuous improvement of security and compliance goes hand-in-hand with a well-developed security plan. Healthcare is a rapidly evolving industry. Your organization's security needs will change over time, just as the technology available to support these needs will continue to evolve. Senior executives and your cloud services provider should review your cloud-computing security plan at least once a year. Plan on revising goals and objectives as needed, reviewing and editing security policies and procedures, and reporting the security and compliance teams' achievements back to your organization.

Half of cloud adopters are hosting clinical applications in the cloud, primarily using

Software as a Service (SaaS). Other common cloud services include Health Information Exchange (HIE), hosting human resources (HR) applications and data, as well as backup and disaster recovery. “Cloud services have been long praised as a tool to reduce operating expenses for healthcare organizations. The data presented in our inaugural survey demonstrates the healthcare industry’s eagerness to leverage this resource,” said Lorren Pettit, Vice President of Market Research for HIMSS Analytics. “With such a positive market outlook, we hope vendors will leverage the business intelligence gleaned from this report, continue working with providers to meet their needs and help healthcare organizations provide the most cost-efficient care.”

> By partnering with cloud providers, healthcare organizations can more readily alter their security plans to support evolving corporate strategies or regulatory requirements.

Although approximately 3 percent of survey respondents expressed a resistance to adopting cloud services due to security concerns, properly managed cloud infrastructure provides better security than most enterprise data centers, applications and IT infrastructure.

Selecting a stable cloud service provider with world-class data centers, enterprise cloud computing infrastructure, application expertise and a proven security methodology will help your healthcare organization reap the financial rewards of cloud computing while implementing a security framework optimized for the requirements of cloud architectures. By partnering with cloud providers, healthcare organizations can more readily alter their security plans to support evolving corporate strategies or regulatory requirements.

For example, NaviSite provides a full suite of reliable and scalable managed services for organizations looking to outsource IT infrastructures and lower their capital and operational costs.

Healthcare enterprise organizations depend on NaviSite for customized solutions, delivered through a global footprint of state-of-the-art data centers. Given that almost all healthcare organizations currently using cloud services plan to expand their use of these tools, the company takes pride in ensuring its enterprise customers’ services are secure and reliable.

For more information, visit www.navisite.com.

SOURCES:

How Cloud Computing is Changing the Health Care IT Industry; Stephanie Ocano - Tech - Sep 16, 2014; http://www.healthcareglobal.com/tech/1630/How-Cloud-Computing-is-Changing-the-Health-Care-IT-Industry

Experts reflect on healthcare cloud data security, complianc; Patrick Ouellette Sept. 11, 2014; http://healthitsecurity.com/2014/09/11/experts-reflect-on-healthcare-cloud-data-security-compliance/

Infographic: Why Healthcare Is Moving to the Cloud; Jasmine Pennic Sept. 25, 2014; http://hitconsultant.net/2014/09/25/infographic-why-healthcare-is-moving-to-the-cloud/80 Percent of Healthcare Organizations Embrace the Cloud; http://www.himssanalytics.org/about/NewsDetail.aspx?nid=82161

From HIE to HR, cloud finding favor; http://www.healthcareitnews.com/news/hie-hr-cloud-finding-favor

Cloud still sparks fear of breaches; http://www.healthcareitnews.com/news/cloud-still-sparks-fear-breaches

About NaviSite:

NaviSite, a Time Warner Cable Company, is a leading worldwide provider of enterprise-class, cloud-enabled hosting, managed applications and services. NaviSite provides a full suite of reliable and scalable managed services, including Application Services, industry-leading Enterprise Hosting, and Managed Cloud Services for enterprises looking to outsource IT infrastructure and lower their capital and operational costs. Enterprise customers depend on NaviSite for customized solutions, delivered through a global footprint of state-of-the-art data centers.

TIME WARNER CABLE Business Class® | NaviSite®

Produced by
HIMSS Media
www.himssmedia.com
© 2014