REDUCING HEALTHCARE COMPLIANCE COMPLEXITY WITH COMMUNITY CLOUDS

MORE THAN DATA SOLUTIONS. **DATA SOLVED.**

CLOUD SECURITY & PRIVACY

Cloud adoption across the healthcare industry is growing, but not without worry for organizations handling sensitive electronic protected health information (ePHI). According to the June 2014 HIMSS Analytics Cloud Survey, 80 percent of healthcare organization respondents reported that they currently use cloud services. For those resistant to moving to the cloud, security concerns was cited as a barrier.

In the healthcare industry, which has some of the most complex IT needs of all industries that exist today, fear of data loss or a breach remains very real. The Ponemon Institute's latest 2014 figures show that the average cost of a data breach to a company was $3.5 million -- a figure that's 15 percent more than what it cost last year. And not all data breaches are the result of malicious intent. Rather, the vast majority is the result of unintentional actions of employees or third-party vendors. From lost or stolen laptops, to misdirected emails and faxes, sensitive ePHI could be potentially exposed at any point in the process.

Remaining secure and compliant is a multifaceted proposition that affects every employee of a health- care facility, every area of its IT system, and all vendors, partners and insurers that work with the healthcare provider. As more data migrates to the cloud, protecting the privacy of patients' ePHI is crucial. As a result, health care providers will need to carefully select a qualified service provider that has a proven history achieving compliance with the Healthcare Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, the American Recovery and Reinvestment Act, and other laws that apply to healthcare organizations.

CONTENTS

STATE OF HEALTHCARE COMPLIANCE

Since the passing of the Privacy of Information Act of 1974, both the U.S. government and the private commercial industry have continued to pass laws and enact self-regulation to protect the confidentiality and integrity of personal or financial information housed on electronic information systems. If a company is compliant with outlined requirements, the expectation is it that it is also secure against threat.

The HIPAA Privacy Rule and Security Rule establishes national standards to protect individuals' medical records and other personal health information. It applies to health plans, health care clearing houses, and those health care providers that conduct certain health care transactions electronically.

HIPAA was sponsored by Senator Ted Kennedy and was enacted by Congress in 1996 to protect health insurance coverage for workers and their families when they change or lose their jobs. The Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifies for providers, health insurance plans, and employers.

The HIPAA Privacy Rule and Security Rule establishes national standards to protect individuals' medical records and other personal health information. It applies to health plans, health care clearing houses, and those health care providers that conduct certain health care transactions electronically. The rule requires appropriate IT security safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosers that may be made of such information without patient authorization. The Rule also gives patients rights over the health information, including rights to examine and obtain a copy of their health records, and to request corrections. Security Rule deals specifically with ePHI.

The Omnibus Final Rule, which took effect on March 26, 2013, outlines changes for covered entities and business associates. This rule now makes business associates and subcontractors of business associates of covered entities directly liable for compliance with certain parts of the HIPAA Privacy and Security Rule requirements. Simply put, the Omnibus Rule puts liability on the provider. Under the old rule, providers were innocent until proven guilty when a breach occurred. However, with the passing of the Omnibus Rule, providers are presumed guilty and will have to prove their innocence. All covered physician practices were required to have updated their HIPAA policies and procedures regarding the Omnibus Rule and implemented accordingly by September 23, 2013.

HIGH COST OF NON-COMPLIANCE

While complying with HIPAA used to be perceived as optional, the HITECH Act of 2009 gave HIPAA compliance some long-awaited teeth. Today, both HIPAA and the HITECH Act have consistent enforcement under the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR).

Not complying with the latest requirements can hold severe ramifications for an organization, as the American Recovery and Reinvestment Act of 2009 established both civil and criminal penalties for failing to comply with HIPAA. For example, in 2014, New York Presbyterian and Columbia University were slapped with the highest monetary payment to date of $4.8 million following a 2010 joint breach report regarding the disclosure of the ePHI of 6,800 individuals, including patient status, laboratory results, vital signs, and medications, among other violations.

THE TIERED STRUCTURE OF CIVIL PENALTIES IS AS FOLLOWS:

HIPAA VIOLATION	MINIMUM PENALTY	MAXIMUM PENALTY
Individual did not know (and by exercising reasonable diligence would not have known) that he/ she violated HIPAA	$100/violation, with an annual maximum of $25,000 for repeat violations (Note: maximum)	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to willful neglect but violation is corrected within the required time period	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation is due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

*Credit: American Medical Association

http://www.ama-assn.org//ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page

CRIMINAL PENALTIES ARE DEALT WITH AS FOLLOWS:

HIPAA VIOLATION	MINIMUM PENALTY
Covered entities whom "knowingly" obtain or disclose individually identifiable health information in violation of the Administrative Simplification Regulations	Up to $50,000 and imprisonment up to one year
Offenses committed under false pretenses	Up to $100,000 and up to five years imprisonment
Offenses committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm	Up to $250,000 and up to ten years imprisonment

Credit: American Medical Association

http://www.ama-assn.org//ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act /hipaa-violations-enforcement.page

CHALLENGES OF ACHIEVING & MAINTAINING COMPLIANCE

Organizations subject to HIPAA are referred to as "covered entities" and organizations delivering services to covered entities are known as "business associates". Per the HITECH Act, these organizations include: healthcare providers such as doctors, hospitals, etc.; healthcare insurance and health plan clearinghouses; businesses who self-insure; businesses that sponsor a group health plan and provide assistance to their employees on medical coverage; and businesses that deliver services to other healthcare providers.

Per these regulatory laws, covered entities and business associates are required to ensure the following safeguards on patient data in order to remain compliant:

- Administrative safeguards to protect data integrity, confidentiality and availability of electronic protected health information (ePHI).
- Physical safeguards to protect data integrity, confidentiality and availability of ePHI.
- Technical safeguards to protect data integrity, confidentiality and availability of ePHI.

One of the main barriers to date has been the simple fact that compliance can be difficult and costly for an organization to achieve and maintain. And for auditors, the process can be very manual and time consuming.

To achieve compliance today, organizations need to be able to fully understand the compliance requirements, which can be difficult when regulations are continually changing or updating. The process typically requires an engineer to configure processes and technology to meet security requirements and additional personnel to conduct risk assessments, document required policy and procedures, and ensure operating procedures meet security requirements. Additionally, achieving compliance often requires an organization to hire a third-party assessor to audit against security standards.

Once an organization has achieved compliance, the next challenge is maintaining compliance. This process often involves ongoing prescriptive operational and security activities, reporting activities, and third-party assessments of operation and security activities.

BENEFITS OF HEALTHCARE COMMUNITY CLOUDS

Under HIPAA regulations, healthcare providers can store Protected Health Information (PHI) in the cloud. To meet this demand, cloud service providers (CSPs) are delivering solutions that can often provide a level of data security that healthcare providers could not achieve on their own. But the healthcare provider must be confident that the CSP is committed to protecting information with at least the same diligence that they would be obligated to exercise if they were doing it themselves[1].

Choosing the right cloud operator platform and hosting provider can help healthcare organizations lower risk, ensure security and privacy of patient data and achieve and maintain compliance. With access to a community cloud focused solely on managing and protecting healthcare data, organizations can find peace of mind even in the face of ongoing and evolving compliance requirement changes.

QTS is taking the complexity out of healthcare compliance with QTS Healthcare Community Cloud (HCC), an Infrastructure-as-a-Service (IaaS) solution that offers healthcare providers and affiliated service companies instant access to a compliant and scalable cloud infrastructure.

QTS HCC is designed specifically for covered healthcare entities and their business associates that must comply with HIPAA and HITECH requirements. Built to meet the specific needs of healthcare organizations, QTS HCC delivers multi-tenant and private cloud capabilities, including the ability to move workloads safely between private and public cloud environments for hybrid cloud deployments. QTS HCC also includes compliant managed services support, which leverages QTS' extensive expertise in managed hosting, colocation and cloud services to deliver highly secure, available, and scalable environments.

[1] *https://www.cdt.org/files/pdfs/FAQ-HIPA AandCloud.pdf*

KEY FEATURES OF HCCS INCLUDE:

- **Instant Access to Compute Resources:** Self-service provisioning of compute and network resources via web portal (or API)
- **High Performance Storage:** Delivered with industry-leading EMC technology, supporting encryption at rest
- **Hybrid Implementation Support:** Customers can easily allocate and manage workloads between QTS HCC and any VMware vSphere® implementation
- **Compliance:** QTS HCC is designed to meet the CSF standards as defined by HITRUST
- **Business Associate Status:** QTS will enter into Business Associate Agreements with all customers of QTS HCC

Built upon the VMware vCloud® Suite, QTS HCC provides reliable, high-performing infrastructure using a platform that includes VMware, EMC and Cisco. QTS HCC easily integrates with private VMware environments to simplify and accelerate end-to-end cloud resource provisioning, delivery, and management while protecting ePHI and meeting the demands of healthcare applications.

QTS' HEALTHCARE INDUSTRY AND CLOUD HERITAGE

With more than a decade of experience delivering cloud services and managed hosting solutions to covered entities, including healthcare providers, insurance and health plan clearinghouses and their business associates, QTS is a trusted cloud operator whose delivery model is oriented around delivering secure and reliable solutions that map our obligations to HIPAA's Security and Privacy Rules. In addition, when appropriate, QTS enters into Business Associate Agreements (BAAs).

Our cloud and compliance experts can also deliver a number of professional services to ensure your infrastructure is compliant.

Additionally, our premium owned and operated data center facilities provide unparalleled security and compliance for entities seeking innovative infrastructure solutions with 24x7x365 support. Our global network of data centers and solutions are backed by two decades of delivering 100% commercial, federal and DoD system compliance accreditations to our customers.

QTS' comprehensive, compliant cloud computing and hosting solutions enable our customers to be confident that they are able to comply with HIPAA/ HITECH obligations.

CONTRIBUTORS

ABOUT QTS | 877.QTS.DATA | QTSDATACENTERS.COM

QTS Realty Trust, Inc. (NYSE: QTS) is a leading provider of secure, compliant data center, hybrid cloud and managed services. QTS features the nation's only fully integrated technology services platform providing flexible, scalable solutions for the federal government, financial services, healthcare and high tech industries. QTS owns, operates or manages more than 5 million square feet of data center space and supports more than 1,100 customers in North America, Europe and Asia Pacific. In addition, QTS' Critical Facilities Management (CFM) provides increased efficiency and greater performance for third-party data center owners and operators. For more information, please visit www.qtsdatacenters.com, call toll-free 877.QTS.DATA or follow us on Twitter @DataCenters_QTS.