EGUIDE – BRIDGING THE GAP BETWEEN HEALTHCARE & HIPAA COMPLIANT CLOUD TECHNOLOGY

Created for Steve Van Tol

Bridging The Gap Between Healthcare & Hipaa Compliant Cloud Technology

Overview

In the healthcare sector, the storing and sharing of sensitive digitized patient data has become a significant undertaking and is a heavy burden on resources. Preparation for a complete conversion from paper medical records to electronic health records (EHR) by 2015 has independent practitioners and small healthcare entities making significant investments in equipment, hardware and software, and tech-savvy personnel.

Rather than focusing on the delivery of core patient care services, they must now worry about IT infrastructure issues, underlying network constraints and data center accessibility as well. This is problematic as very few medical offices or small health service organizations can afford to employ dedicated IT staff.

In this context, it is obvious that cloud-based solutions, which consolidate and outsource computing resources to external entities, would provide substantial relief to healthcare service providers. Data stored in the cloud is available on-demand and requires no expensive equipment, physical home or hired staff to manage and maintain it.

But while other business sectors have fully embraced the cloud for cheaper, more flexible, scalable and secure computing, many in the healthcare sector have yet to entertain putting patient data into the cloud. HIPAA-driven security and privacy concerns have been a serious deterrent.

This is about to change. Recent modifications to the HIPAA Privacy, Security, Enforcement and Breach Rules have made it clearer that data center operators are to be classified as business associates under HIPAA. This means cloud-service providers are required by law to report and respond to data breaches and uphold their obligation to properly protect and secure patient info.

These modifications are a game changer because they now assure covered entities such as doctor offices, hospitals, and health insurers that they can remain HIPAA compliant while adopting cloud technology.

EGUIDE – BRIDGING THE GAP BETWEEN HEALTHCARE & HIPAA COMPLIANT CLOUD TECHNOLOGY

Cloud Computing in Healthcare Sector Projected to Grow

According to recent report by the research firm Markets and Markets, although the healthcare sector has been notoriously slow when it comes to adopting new technology trends, the cloud computing market in this sector is projected to grow to $5.4 billion by 2017.

Breaking Down HIPAA and the Cloud

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was upgraded in 2009 with the Health Information Technology for Economic and Clinical Health (HITECH) ruling addressing the growing use of digitized medical records. HITECH was introduced to provide federal funding to deploy EHR and establish a protocol for protecting the electronic storage and transmission of Protected Health Information (PHI).

[PHI is defined as any information obtained, used or disclosed in the course of providing a healthcare service--treatment, payment, operations or medical records--that can be used to identify an individual.]

Compliance with HIPAA requires the reporting of any potential unauthorized PHI access. Because any impermissible access, use, or disclosure of PHI can severely damage an organization's reputation, as well as levy penalties varying from $100 to $50,000 for first time offenders, it is understandable that many in the healthcare industry have chosen to avoid migrating patient data to the cloud unless they're absolutely certain that a cloud-service provider (CSP) is HIPAA compliant.

Cloud-Service Providers as HIPAA Business Associates

Over the past five years, there has been much confusion whether cloud-service providers were classified as business associates (BAs) under HIPAA. The Department of Health and Human Services holds BAs accountable for certain required privacy and security obligations to protect PHI data, upholding them to a signed Business Associate Agreement (BAA). If confidential health data is compromised, the Associate is liable for responsibilities on their end.

The HIPAA privacy rule defines a BA 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."

Since most CSPs "maintain" PHI on behalf of either the covered entity or another BA that subcontracts them,

one would assume they'd be deemed a BA themselves. But that hasn't always been the case due to some ambiguous language that originally accompanied the regulation, language that was only just recently modified to expand the scope of BAs as defined by HIPAA.

The Old Rule...

"Data transmission organizations that the Act requires to be treated as business associates are those that require access to protected health information on a routine basis. Conversely, data transmission organizations that do not require access to protected health information on a routine basis would not be treated as business associates."

As you can see, this language easily leaves "access on a routine basis" up to interpretation. For instance, although it states that HIPAA requires those accessing PHI data on a routine basis be treated as BAs, some CSPs felt they were mere "conduits" of protected data – not very different than courier services or postal services, having only random or infrequent access to public health information as they transport/share it with others. These CSPs would often argue that a signed BAA wasn't necessary, thus avoiding the added due diligence or security control requirements and liability.

Take a high-volume Platform-as-a-Service (PaaS) for example. Here the CSPs primary role is to provide storage services that enable the covered healthcare entity's staff, such as a doctor's office, to routinely look at data stored remotely. While the CSP providing the PaaS bears responsibility for maintenance and upgrades to the hardware, software and the operating system, they don't touch the actual PHI data all that much. Therefore, a CSP offering PaaS doesn't necessarily have the same level of PHI access as a cloud provider using Software-as-a-Service (SaaS) who must grant their personnel daily access to PHI.

A similar argument could be made for a CSP who maintains encrypted PHI for a covered healthcare entity but doesn't hold the encryption key.

This uncertainty was the reason for much of the healthcare sector's reluctance to take to the cloud. If a cloud-service provider (CSP) didn't feel the need to sign a BAA, and the patient info they managed was breached, the covered healthcare entity, not the CSP, would be fined.

EGUIDE – BRIDGING THE GAP BETWEEN HEALTHCARE & HIPAA COMPLIANT CLOUD TECHNOLOGY

The New Rule...

"A data storage company that has access to protected health information (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis. Thus, document storage companies maintaining 26 protected health information on behalf of covered entities are considered business associates; regardless of whether they actually view the information they hold. To help clarify this point, we have modified the definition of "business associate" to generally provide that a business associate includes a person who "creates, receives, maintains, or transmits" (emphasis added) protected health information on behalf of a covered entity."

The new HIPAA Omnibus Rule further clarifies that BAs and subcontractors of BAs are directly liable for compliance with certain HIPAA Privacy and Security Requirements. This has calmed skeptics, resulting in a healthcare industry now actively looking to cloud-based solutions.

How Cloud Computing Enables Industry Advancements

When it comes to staying on top of industry trends, those in the healthcare sector utilizing cloud computing will undoubtedly have an advantage over those slow to adapt to change. The Internet is more widely used now by both patients and those providing health services.

Today's patient desires anytime/anywhere access to health-related information and physicians may need access to digitized health data such as MRI scans, ultrasound images, or mammograms. Patient information must also be accessed for clinical decision-making such as potential prescription drug interactions or the American Recovery and Reinvestment Act of 2009 (ARRA) funded community health information exchanges (HIEs) that enable health providers and insurers to share a patient's medical records with his or her permission. The cloud supports all of these.

In many ways, cloud computing levels the playing field as its affordable benefits are available to anyone from a small physician's office or non-profit to large organizations or insurers. This fosters an all-inclusive collaboration that isn't restricted to only large institutional players.

EGUIDE – BRIDGING THE GAP BETWEEN HEALTHCARE & HIPAA COMPLIANT CLOUD TECHNOLOGY

Major Benefits of the Cloud for the Healthcare Sector

- **Security** – Ironically, the biggest concern most healthcare entities have about taking to the cloud is one of its biggest strengths. Recent updates have made CSPs as responsible and liable for HIPAA compliance as the healthcare institutions that hire them. CSPs must ensure that data is encrypted, backed up, easily recoverable, and secured with permission-based access.

- **Costs** – Reduced costs are an incentive for healthcare entities to take to the cloud. Costs are dramatically cut since the cloud moves everything into a virtual environment, eliminating the need for costly hardware, software, maintenance, data center space, and IT labor. Pay-as-you-use fees requiring little-to-no capital investment replace these often overwhelming up-front capital expenses.

- **Scalability** – With the 2015 EHR conversion deadline nearing, and the fact that health service providers are generally required to maintain patient medical records for at least six years, it's easy to anticipate that managing such a high volume of patient data will inevitably stress any on-site IT infrastructure. But the cloud presents a scalable alternative where additional server or storage capacity is available as needed.

- **Mobility** - The cloud improves a physician's ability to remotely access readily available patient information. This enables even the busiest physician to review a patient's medical records or test results even after they leave the office.

- **Sharing** – Cloud computing keeps physicians better connected to not just their patients but their colleagues as well. Patients will notice benefits to medical professionals being able to share patient information online – for example, referrals to specialists will be more timely, there will be less paperwork to fill out with each office visit, and no unnecessary repeat diagnostic tests.

Are You Ready for This Transition?

The transition to cloud computing is underway in the industry. For healthcare service providers, it is no longer a question of if they will transition to the cloud, but when they can start benefiting from its potential savings and all of its capabilities.

Healthcare is a heavily regulated industry and cloud computing will continue to evolve to meet the industry's growing security requirements and regulatory mandates. Many legitimate CSPs familiar with the healthcare sector already have strict security protocols in place to comply with regulations and will not hesitate

to sign a BAA when asked. It is best to choose a CSP cautiously. Avoid any CSP who refuses to sign a BAA and carefully evaluate even those who do to get a feel for their stability, level of service, and delivery on promises.

Taking care of people - not your IT infrastructure - is your core service. Why not put the money being spent right now on hardware, software and equipment back into patient care while actually strengthening patient data integrity and security? Contact us today if you'd like to learn more about HIPAA compliant cloud-based technology.

For Additional Information Please Contact
Steve Van Tol
steve.vantol@jcmr.net
T: 704-707-3333 x3008
5950 Fairview Road Ste 140, Charlotte, NC, 28210