EXECUTIVE REPORT

CyrusOne

Why Healthcare Providers Seek Out New Ways to Manage and Use Big Data

The HIPAA and HITECH acts, alongwith the Affordable Care Act,are changing the face of the healthcare industry. These government reform efforts are aimed specifically at using technology to improve hospital efficiency and patient care. As a result,the government has establishedregulatory standards for everything from how electronic health record (EHR) systems are used to how hospitals protect patient data and privacy.

The Healthcare Data Deluge

This technology-centered approach to healthcare represents a major shift from historical models. While medical technology has always been vital to care goals, information technology (IT) has been handled conservatively to avoid any risk. Over time, this approach has left many hospitals falling behind from a technological perspective, but the industry is now working to catch up.

The influx of IT creates challenges in both the operational and fiscal layers of hospitals, forcing them to deal with the emergence of new regulatory compliance, costs and big data-related issues. Individually, these issues are all problematic for hospitals. Facing all of them at once can be extremely daunting. Thus, third-party help in the form of colocation and data center services is emerging as a key strategic enabler across the healthcare industry.

Hospitals have always dealt with large amounts of information, but the transition from paper to electronic records emphasizes not only the amount of data being dealt with, but the amount of information that should be used. With paper records systems in place, hospitals, physicians' offices and clinics maintained large quantities of files with individual patient data and only shared information when necessary.

Healthcare reform is focused on not only improving how hospitals manage data, but how they use it. More collaboration is necessary, data sharing is becoming critical, and community-care ideas are taking shape. This creates new challenges in a wide range of operational areas, including data protection, regulatory compliance and IT management.

Dealing with Data Protection

Regulatory compliance and data protection are inherently linked, but there are facets of data protection that are vital regardless of what HIPAA standards promote, making a separate discussion of the two areas essential. From a purely operational standpoint, hospitals face a unique security challenge because they not only have to deal with the usual data protection considerations; they also face unique patient privacy challenges.

On one hand, physicians need access to patient data to do their jobs while on the other, not every doctor in a care facility can have the same access to data. Glenn Mamary, chief information officer (CIO) CIO of Hunterdon Healthcare System, says his health network had experienced this problem in the past, as a data storage model that was open to physicians led to some doctors looking at patient data that they did not have to view.[1] Therefore, Mamary developed a system that tightly protects who can access what data with sophisticated passwords, withan override capability that physicians can use in the event of an emergency.

These types of issues lead to major questions about where care providers should store data and how they should protect it. HIPAA guidelines provide the initial guidance that hospitals need in this area.

Addressing HIPAA

HIPAA regulations set a foundation upon which hospitals can build their data protection and privacy policies. However, HIPAA is not a handbook or even a set of best practices. The problem is not that the guidelines themselves are flawed, but the industry is so diverse that HIPAA aims to establish broad common goals. The standard is not designed, in most areas, to tell care providers how to achieve the end results. Hospitals have to evaluate their own operational and technological capabilities and navigate the regulatory climate on their own to achieve success in data protection.

For example, HIPAA regulations mandate the accessibility of certain types of patient health information at all times to ensure continuity of care. This means while most businesses can focus on IT disaster recovery during an outage, hospitals have to first ensure they have business continuity plans in place before moving on to recover normal functionality. How hospitals accomplish this is up to them. This is one area where colocation can help by keeping data accessible in a remote location.

The other challenge when dealing with HIPAA is it does not only apply to hospitals and care providers; it also impacts any business partners or organizations handling patient data. Healthcare industry companies are responsible for ensuring they only work with business partners that can meet HIPAA requirements.

These factors are combining to put a significant burden on hospitals because IT functionality plays a central role in supporting HIPAA compliance. Furthermore, HIPAA and the HITECH acts deal primarily with protecting patient data and keeping it private; attesting for meaningful use, which is the central theme of healthcare reform, adds another level of challenges.

[1] Schetman, Joel. "Healthcare CIOs Must Walk Fine Line Between Doctor Access and Patient Privacy." The Wall Street Journal. N.p., 15 Aug. 2012. Web. 03 Dec. 2012. http://blogs.wsj.com/cio/2012/08/15/healthcare-cios-must-walk-fine-line-between-doctor-access-and-patient- privacy/.

Meaningful Use Attestation

While HIPAA is one of the most frequently discussed elements of healthcare reform, meaningful use is the central point around which HIPAA revolves.

Meaningful use standards are clear and actionable care goals set forth by the government to ensure consistently high-quality care around the country. Guidelines range from using technology to enable data sharing and fuel collaboration, to asking patients specific questions during consultations to better evaluate their general health. HIPAA is in place to ensure that patient data is protected while the reform efforts included in meaningful use are implemented.

At its core, meaningful use standards are focused on encouraging hospitals, physicians' offices and clinics to not only deploy EHR systems, but to allow increased IT functionality to permeate operations to such an extent that it leads to care improvements. The standards are about effectively using the EHR infrastructure. This requires innovation on three levels: internally, within a care network and within the larger community.

Internally, effective EHR deployment in hospitals hinges on being able to share data between labs and other departments and patient care areas. This ensures physicians have the information they need when they need it, and that the information is accurate and includes any supplemental details that can improve care. This process, is heavily dependent on robust server and storage systems that can handle high-density operations and function reliably.

Meaningful use also encourages better data sharing and collaboration within a health network. A hospital physician specializing in a certain type of care can use EHRs more meaningfully when he or she has access to the same patient data as a primary care physician. The process of sharing data across EHR systems hinges on advanced IT capabilities that not only enable this type of functionality, but also allow for effective security and privacy measures.

These initial forays into big data expand exponentially when getting into community health. Championed by accountable care organizations but essential in the industry as a whole, community health processes involve analyzing patient data corresponding to individuals within a town, county, state or even country, using that information to identify individuals who may be at risk.

While community care could prove vital in supporting healthcare reform efforts, it also puts a considerable burden on the data center. Any operational practice involving big data or similar types of processes hinges on aligning storage and server setups to work effectively with each other. The performance challenges, however, are only part of the problem.

Protecting patient data is also a vital consideration. Data center protection is becoming a critical issue in healthcare and it is a challenge that involves a combination of access control, cybersecurity, uptime and facility security considerations. These are all things hospitals have not had to deal with to this degree in the past and may not be able to afford to handle now.

Considering the Cost Side of Meaningful Use

Implementing the IT infrastructure needed to achieve even the first stage of meaningful use is incredibly expensive, and that only addresses initial EHR implementation and internal integration. Expanding to the external and community care goals that could drive long-term gains for hospitals requires even more hardware. Government reform efforts are built to make up for this problem, as hospitals that can attest for meaningful use can obtain stimulus funding. Over time, organizations that do not attest for meaningful use will face repercussions in the form of adjustments to Medicare and Medicaid reimbursements.

While the funds available for achieving meaningful use provide some help for hospitals, they are dwindling quickly and are proving to be insufficient for covering the cost of more robust technological deployments. This is leading to the emergence of major roadblocks across the industry, as many hospitals are trying to comply with government reform goals but are in a financial position that limits innovation.

As a result, many CIOs are beginning to seek more creative ways to deploy and manage the IT infrastructure needed to support operations.

Meaningful use is only one side of the cost equation. The amount of funding needed to support attestation is significant, but so is the potential loss for hospitals unable to comply with meaningful use or HIPAA regulations.

Dealing with Regulatory Costs

Hospitals failing to attest for meaningful use have to deal with Medicare and Medicaid reimbursement cuts, which could severely impact the revenues of many care centers. Unexpected costs caused by noncompliance with HIPAA standards can also create problems. The costs of any type of outage or data-loss incident, while substantial, are almost impossible to clearly identify.

This difficulty is because outages involve several variable conditions. A data breach of any sort can lead to fines, reputational damages, fees associated with credit card tracking for those affected by the event and a variety of other conditions. As a result, hospitals have to invest heavily in security and data protection to avoid HIPAA-related issues and ensure patient data privacy.

Dealing with Complexity and Cost

The myriad of factors that come together in HIPAA, the HITECH acts, the Affordable Care Act and meaningful use attestation are pushing healthcare into a new era of dependence on IT functionality. Furthermore, these problems are being exacerbated by the growing importance of cloud computing, mobility and other emerging technologies taking hold in the sector.[2]

In response, healthcare CIOs have to find ways to improve functionality substantially while also reducing costs to a meaningful extent. This is an area where colocation and similar data center services pay major dividends.

Using Colocation to Reduce Cost and Complexity

One of the core gains associated with colocation is the elimination of capital costs needed to build a new data center. While this benefit is clear, healthcare organizations benefit even more from the holistic vision of a well-designed colocation strategy.

When companies use colocation effectively, they gain access to more robust and sophisticated data center resources than they can usually manage on their own. However, they do this without giving up control of their IT systems.

Working with a hosting provider that can operate within HIPAA and HITECH regulations positions hospitals to simplify the process of complying with regulatory standards by making data center systems more reliable, accessible and redundant.

Colocation provides a foundation for the high-density server and storage environments needed to deal with the data-related challenges facing hospitals.

Colocation also helps hospitals by providing them with facility and management improvements. A colocation data center designed for healthcare can offer robust network and physical security, as well as access control measures within the data center, to ensure regulatory compliance. At the same time, power and network redundancy combined with the flexibility offered by colocation providers makes the service model much more reliable than premise-based data centers.

Scalbility, Security and Reliability

Using Colocation to Enable Scalability

Another key need for hospitals is scalability. As EHR functionality grows and hospitals deal with more IT systems, they need a data center that can adapt to shifting operational requirements. The leasing model used by colocation vendors provides flexibility from a cost standpoint. Facility design within colocation centers allows for scalability from an IT perspective.

Using Colocation for Security and Reliability

Security and reliability play major roles in healthcare, especially as regulatory guidelines specifically address such issues.

Protecting data is an incredibly important consideration for hospitals because the costs of a data breach can escalate quickly. Colocation improves security and privacy on multiple levels. On a physical layer, colocation facilities provide access control features that tightly regulate who can enter the building, access the data center floor, maintain equipment, and actually view server environments.

This security not only keeps data protected from physical theft; it also provides the privacy-related nuances needed to ensure people only view the information they are authorized to see. Secure networks, which play a major part in colocation services, add a key layer of logical protection to patient data.

Reliability is not an area where hospitals can afford to take risks. Lives can be lost if IT systems go down and patient data becomes unavailable. Most colocation facilities feature redundant power supplies and network systems to ensure constant availability. Furthermore, providers can house client data in multiple facilities, ensuring that data is available even if there is a problem at one of the data centers.

While the IT innovation needed to support HIPAA, the HITECH acts, the Affordable Care Act and meaningful use standards is daunting, HIPAA-compliant colocation services offer the cost-efficiency and performance needed to help hospitals comply with government reform efforts, contributing to the greatest gain of all – more lives saved through better care.

Summary

CyrusOne's HIPAA-compliant colocation facilities feature best-in-class security, scalability and reliability, helping hospitals reduce costs and complexity and simplifying compliance with regulatory standards. In addition, CyrusOne's industry- leading interconnection platform offering allows healthcare organizations to seamlessly share information with business partners, content providers, networks, carriers and other entities via the CyrusOne National Internet Exchange (IX).

About CyrusOne

CyrusOne specializes in providing highly reliable, flexible and scalable enterprise data center colocation that meets the specific needs of customers across its broad portfolio of carrier-neutral data center facilities in the United States, Europe, Asia and Latin America. CyrusOne employs its Massively Modular® engineering and design approach to optimize design and construction materials sourcing and enable just-in-time data hall inventory to meet customer demand. The company engineers its facilities with redundant power technology, including an available 2N architecture.

CyrusOne customers can mix and match data centers to create their own production and/or disaster recovery platforms by combining facilities via the low-cost, robust interconnectivity provided by the CyrusOne National Internet Exchange (IX).