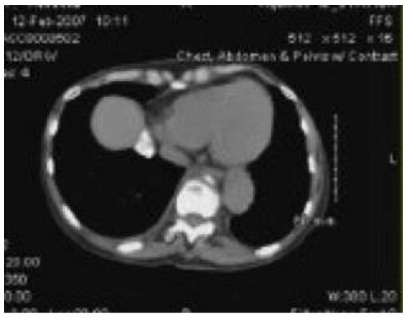
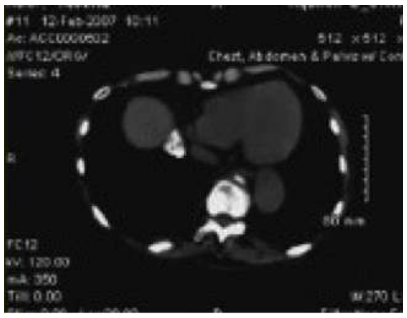
CyrusOne

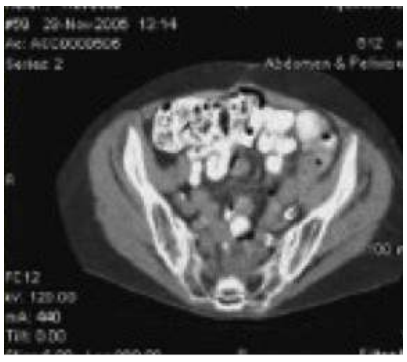
Executive Report

Tackling the Critical IT Challenges of Healthcare Reform

Many healthcare providers are turning to colocation providers like CyrusOne, which provides a robust, all-encompassing information technology (IT) infrastructure environment much more efficiently and cost-effectively than most hospitals can.







How Healthcare Organizations are Helping Growing Complexities

The healthcare industry is at a crossroads. While patient care remains a top priority for all organizations across the industry, HIPAA regulations, HITECH compliance and myriad other mandates are contributing to an increasingly complex business environment.

The changes have been particularly hard on independent physicians' offices. No longer able to operate feasibly as solo entities, these organizations are being folded into larger hospitals and medical centers.

These organizations must decide the best ways in which to handle their critical IT infrastructure. Healthcare leaders must determine whether to outsource their data centers to a colocation provider or spend the resources and time building such centers from the ground up – and staffing and maintaining them over time.

The Need for Robust, Reliable Data Centers is on the Rise

HIPAA and HITECH are two of the many new laws complicating the healthcare landscape. Regulatory standards governing how electronic health record systems are used and how hospitals protect patient data and privacy can only be handled through technology that improves hospital efficiency and patient care.

The need for efficient, productive, reliable data centers is only exacerbated by the fact that the federal government is playing an increasingly active role in the delivery of healthcare.

Healthcare facilities, hospitals, medical centers and solo providers rely heavily on technology to meet the growing need for compliance standards within their industry. Also driving the demand for robust, reliable data networks are ever-changing processes such as electronic health records (EHRs), wireless, digital imaging and other advanced technologies.

The need to create capable data ecosystems has never been as critical as it is right now. Along with delivering quality patient care, providers must also meet compliance mandates, protect client data, address patient safety and satisfaction, and manage a growing volume of information. Making the situation even more challenging is the fact that these goals must be achieved in an IT environment with optimal uptime and maximum security.

By delivering a flexible, reliable data center ecosystem in a secure, cost-effective manner – and requiring no long-term IT maintenance or security on the part of the hospital – CyrusOne helps clients improve utilization, lower expenses, and get up and running quickly and efficiently.

CyrusOne's data centers are engineered to deliver top-tier availability backed up by 100% uptime service-level agreements (SLAs). Our data centers are built with up to 2N redundancy of mechanical and electrical systems for a highly resilient environment that's perfectly suited for the healthcare industry.

Addressing the Critical Challenges of Healthcare Reform

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

Data security is also a rising concern for healthcare organizations. From a purely operational standpoint, both hospitals and physicians' offices face a unique security challenge because they not only have to deal with the usual data protection considerations, but they also face unique patient privacy challenges.

On one hand, physicians need access to patient data to get the job done, while on the other, not every doctor in a care facility can have the same access to data.

Glenn Mamary, chief information officer (CIO) of Hunterdon Healthcare System, says the 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, with an override capability that physicians can use in the event of an emergency.

Mamary's issue with his data storage model is exactly why more healthcare organizations view colocation as the right solution. After all, what company really wants to reach far out of its core revenue-generating activities to spend thousands of dollars and hundreds of hours of time establishing and running a data center?

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

Interconnected, Secure Data

"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 the 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 to be put into place.

The initial forays into big data have grown exponentially in the community health field. 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 and using that information to identify individuals who may be at risk.

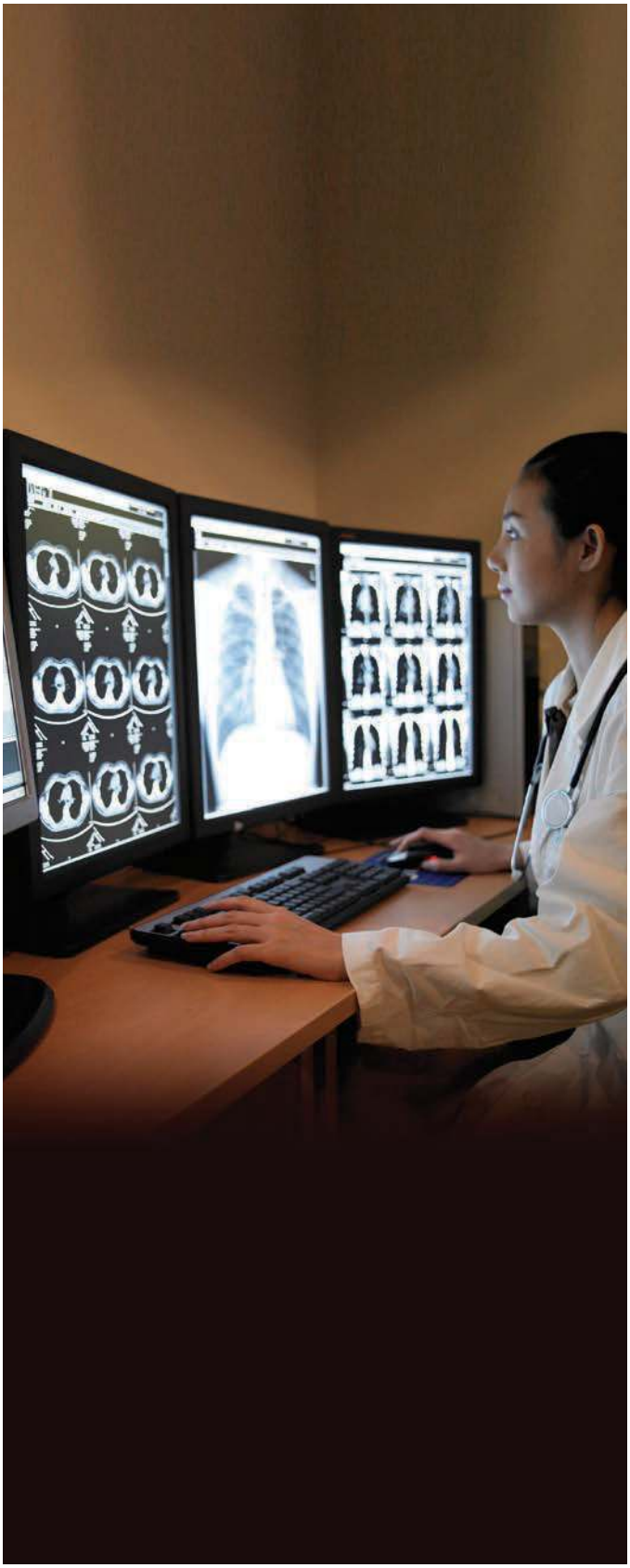
While community care could prove vital in supporting healthcare reform efforts, it also puts a considerable burden on a data center. Any operational practice involving big data or similar types of processes hinges on aligning storage and server setups to work effectively in conjunction with each other. 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, cyber security, 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.

Performance infrastructure and secure patient data needs dictate that data centers provide a cohesive combination of access control, cyber security, uptime, and facility security considerations. A colocation provider like CyrusOne can create solutions to manage these evolving requirements.

Meaningful Use Attestation

HIPAA revolves around meaningful use standards, clear and actionable care goals set forth by the government to ensure consistently high-quality care around the country. These guidelines range from using technology to enable data sharing and collaboration, to asking patients specific questions during consultations to better evaluate their general health.



To ensure that patient data is protected, HIPAA meaningful use standards encourage hospitals, physician offices and clinics to not only deploy EHR systems but to allow increased IT functionality to permeate operations such that it leads to care improvements. Effectively using the EHR infrastructure requires innovation on three levels: internally, within a care network and within the larger community.

Internally, successful EHR deployment in hospitals hinges on effective data sharing between multiple patient care areas so that physicians and staff have accurate and detailed information to improve and streamline patient care. This process is heavily dependent on robust, reliable server and storage systems that can handle high-density operations.

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 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 do acknowledge these challenges 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 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 hospitals try 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 Complexity and Cost

The convergence of HIPAA, the HITECH Act, 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.

Healthcare CIOs have to find ways to improve functionality substantially while also reducing cost. This is an area where colocation and similar data center services pay major dividends.

One of the core gains associated with colocation is the elimination of capital costs needed to build a new data center. While this advantage 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. When working with a third-party hosting provider, capable of complying with HIPAA and HITECH regulations, hospitals can 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 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.

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.

Finding Security and Reliability in Colocation

As the IT environment becomes more complex for hospitals – and as more independent physicians' offices join forces with their larger counterparts – the need for interconnected, robust data centers will only grow. Add increasingly stringent regulatory guidelines to the mix and issues like data protection, consumer privacy and access control become even more crucial.

Colocation improves security and privacy on multiple levels. On a physical layer, such facilities provide access-control features that tightly regulate who can enter the building, who can access the data center floor, who can maintain equipment, and who can actually view server environments. This security not only keeps data protected from physical theft: it also provides the privacy-related nuances needed to ensure that 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.

Summary

While the IT innovation required to support HIPAA, the HITECH Act, the Affordable Care Act and meaningful use standards is daunting, HIPAA-compliant colocation providers 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.

Agile, experienced and well-positioned to accommodate the exploding requirements of the healthcare industry, CyrusOne's data centers support secure and resilient IT deployments, best-in-class redundancy in power and cooling architecture, superior electrical and mechanical systems with unparalleled interconnection and connectivity. CyrusOne's National Internet Exchange (IX) allows customers to seamlessly share information with business partners, content providers, networks, carriers and other entities via a robust and secure cloud.

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 and Asia. 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).

About the Author

Scott Brueggeman

Chief Marketing Officer

With more than 20 years of combined experience in data center, telecom and internet marketing, Scott oversees global marketing strategy for CyrusOne. His initiatives have earned CyrusOne notable marketing honors, including the BMA Gold Tower Award, Gold Stevie Award, and B2B Marketing Campaign of the Year by the Business Marketing Association.

Before joining CyrusOne in 2012, Scott's experience spanned leadership roles in Fortune 100 firms, mid-size internet marketing companies, and several high-growth organizations. As Vice President of Marketing at CoreLink Data Centers (since acquired by Zayo), he launched new brand architecture and integrated marketing initiatives, which received awards of distinction from the American Marketing Association and Business Marketing Association.

CyrusOne
Built for Tomorrow. Ready Today.