virtustream

Whitepaper

Healthcare and the Adoption of Digital Health Solutions in the Cloud

A fundamental change is underway in the healthcare industry. Hospitals, Ambulatory Care Centers and Physician Clinics are undergoing a digital transformation, integrating their electronic health record (EHR) platforms with new patient engagement systems and emerging precision health platforms. They have three primary goals: improve the quality of care, empower patients to take control of their health, and reduce the cost of operations.

The increasing complexity of the healthcare IT landscape is driving healthcare organizations to consider new options that can embrace digital strategies and increase agility while reducing costs. Security mandates are growing due to the upswing in cyber attacks on health providers and the protection desired for protected health information (PHI). While on-premises solutions offer perceived advantages, industry leading healthcare providers are closely examining enterprise cloud options for hybrid and off-premises deployment models that meet or exceed high security and compliance requirements, while offering utility-based billing and cloud flexibility. For enabling digital healthcare transformation, enterprise cloud services provide a host of avenues to support healthcare providers.

Digital Health Solutions. What do They Provide?

As with any new technology, digital health solutions are not a panacea for healthcare's IT complexities. They need to be accompanied by careful planning and operational management in order to be implemented successfully and guarantee the best outcomes.

In today's market, there are many well-established EHR solutions. Among the most popular in the field are Epic, Cerner, MEDITECH and Allscripts. With these EHRs and supporting healthcare applications, IT departments can create ecosystems of patient care systems. Enterprise cloud services that include security and compliance, utility billing and high availability guarantees enable healthcare IT to respond quickly while delivering greater accuracy. IT departments can scale up appropriately to meet growing business requirements, rapidly deploy new infrastructure to support new applications, and connect operational IT systems like EHRs with patient engagement systems and precision medicine platforms. In today's market, a healthcare system with a single EHR is a rarity and multiple digital health solutions can add complexity and resource challenges to the environment.

By implementing a new patient-centric digital strategy, providers and clinicians can give their patients top-of-the-line care and make the appropriate medical decisions by having a complete set of information on hand.

Healthcare IT is Trending Towards the Cloud

The digital transformation is well underway in the healthcare market. In 2015, approximately 95% of

hospitals possessed certified EMR/EHR technology, increasing from 72% in 2011[1]. Alongside this growth in certified EHR technologies and systems, digital picture archiving and communication systems (PACs) are steadily migrating to vendor-neutral archive systems (VNAs), establishing a gateway to tiering and cloud solutions. According to a Market and Markets report, the global medical image management market is expected to grow at a rate of 6.5% annually from 2016 to 2021[2]. Additionally, the U.S. Food and Drug Administration's (FDA) recent approval the first whole slide imaging (WSI) system that allows for primary diagnosis based on review and interpretation of digital surgical pathology slides will drive a dramatic increase in data storage requirements in the very near future[3].

Emerging precision medicine systems are coming to market, connecting consolidated patient data with analytic systems and facilitating clinicians to improve quality while lowering the cost of patient care. Today the ability exists for a doctor in Kansas to compare the treatment of his or her diabetic patient to those of diabetic patients across the United States, evaluate the impact of different treatment regimens, adopt a specific treatment plan and, going forward, track that patient's daily adherence to the plan – all on a mobile device.

To enable this transformation, healthcare decision makers will be required to redirect resources that today are engaged in "keeping the lights-on" aspects of the primary IT infrastructure. By doing so, infrastructure can be modernized to free up staff to innovate rather than maintain the day-to-day operations. A hybrid cloud model can be leveraged to manage cloud environments and supplement in-house infrastructure and expertise to manage solutions or application delivery, as well as address the growing risk associated with increasingly complex cybersecurity pressures.

Cloud adoption for health IT is accelerating as more healthcare providers are transitioning their existing IT infrastructure, including their EHRs, to a managed environment. Global healthcare cloud spending on services and products is expected to grow 20.1% annually between 2014 and 2020. These expenditures are projected to reach an estimated $12.6 billion in 2020[4]. Additionally, the increasing availability of healthcare-specific cloud services and vendors will improve access to cloud systems and provide more options directly focused on meeting the demands of the healthcare industry. According to an International Data Corporation (IDC) study, U.S. healthcare providers reported in 2016 that over 40% of their spending would go towards managed hosting and Software as a Service (SaaS) offerings[5]. Along with this trend, a Gartner report indicates that healthcare providers' growing infrastructure, system and support requirements, in conjunction with tight budgets and IT staffing issues, are driving towards a hybrid IT environment where the cloud will play an increasing role[6]. Many providers choose to off-load portions of their IT environment to a hybrid deployment as opposed to a full-scale cloud as a way to remain comfortable still maintaining in-house infrastructure.

Security and Compliance are Driving Managed Cloud Deployments

Healthcare is lagging behind other industries in cloud adoption, with data privacy and data security being cited as leading factors. In the first three months of 2017, over 78 data breaches have been reported to the US Department of Health & Human Services "wall of shame"[7]. One of the primary responsibilities of healthcare

1 Crandall, Mary Anne. "Electronic Medical Records 2016." Kalorama Information. April, 2016
2 Market and Markets. "Medical Image Management Market by Product (PACS (Departmental (Radiology, Cardiology), Enterprise), VNA (On-premise, Hybrid, Cloud, Multi- department, Multi-site, ISV), AICA) & End user (Hospitals, Diagnostic Imaging Centers, ASC, CRO) - Forecasts to 2021." December 2016.
3 Food and Drug Administration. "FDA allows marketing of first whole slide imaging system for digital pathology." April 12th, 2017. <https://www.fda.gov/NewsEvents/Newsroom/ PressAnnouncements/ucm552742.htm>.
4 Persistence Market Research. "Global Market Study on Healthcare Cloud Computing: Hybrid Clouds to Witness Highest Growth by 2020." 2015.
5 Hanover, Judy. "Business Strategy: Trends and Opportunities in the U.S. Healthcare Provider Market." January, 2016
6 Pessin, Gregg and Barry Runyon. "Market Guide for Cloud Service Providers to Healthcare Delivery Organizations." November 16th, 2016.
7 U.S. Department of Health and Human Services Office for Civil Rights. "Breaches Affecting 500 or More Individuals." <https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf>.

providers today is maintaining the security of protected health information (PHI), with strict adherence to compliance frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). In the current state of today's healthcare industry, security mandates are becoming stricter and more complicated due to a significant upswing in digital attacks aimed at PHI. This healthcare data is viewed as up to 10 times more valuable than other forms of personal information when sold on the black market. When debating the use of an off-premises or hybrid cloud, these regulatory risks are taken into critical consideration. And quite often, executives feel as though PHI would be safer on-premises rather than with a cloud provider.

Enterprise-class cloud providers in the market have strict guidelines and protocols when it comes to data protection. In many cases, cloud deployments can be as safe as or safer than on-premises implementations, depending on the role security plays for the cloud provider, security technologies used and guarantees provided. Cloud providers must operate their security and compliance systems at scale. They must always be up-to-date on the latest regulatory requirements, minimize the risk caused by human error, and be able to provide audit and tracking for the entire environment. They also need dedicated teams focused on end-to-end security. Clients then get the benefit of large-scale, highly compliant, highly automated systems that would be too costly to purchase and impractical to manage by an individual customer. Typically, their customers also require contractual guarantees on the security of their data, and the adherence to compliance requirements, including high dollar penalties attached. Only recently, cloud service providers (CSPs) have begun to understand the gravity of business associate agreements (BAA), which is a contract between a HIPAA-covered organization and a HIPAA business associate, and compliance requirements.

Healthcare IT security teams often lack the tools and time for a comprehensive, multi-dimensional end-to-end strategy to protect patient data. Moreover, without an end-to-end strategy, healthcare providers can suffer deficiencies in not just data protection, but also threat detection, identity access, and management of endpoints and devices. Government regulations which frame the day-to-day compliance requirements of digital health solutions change regularly. In some regions, government mandates for EHR systems present an extra level of urgency for understaffed and underfunded healthcare IT departments. Even the most experienced security specialists struggle to keep up with the requirements of HIPAA compliance.

By transitioning to a managed cloud service solution, healthcare providers can ensure an in-depth defensive security model to secure patients' private information. In addition to compliance with regulatory frameworks, a cloud service's ability to protect sensitive patient information is an increasingly crucial reason why healthcare organizations are looking towards the cloud. With role-based access controls, multi-factor authentication, data encryption at rest and in motion, multiple levels of threat detection, and a myriad of other security tools, cloud providers have layers-upon-layers of security that can meet the rigorous requirements of the healthcare industry.

Cloud Enables Healthcare Transformation

While there are plenty of drivers within the IT environment of a healthcare provider to adopt a cloud solution, there are also several factors inherent to a cloud offering make this very model attractive for more widespread adoption. A cloud solution can enable the transformation of hospitals, ambulatory care centers and physician clinics by providing benefits that cannot be delivered through an on-premises deployment.

A cloud deployment can respond to the changing budgetary needs of a healthcare provider, shifting budgets from capital to operational. Deployment of a

cloud environment not only may be less expensive than an on-premises option, but it can also provide a greater time-to-value for the investment. This value is seen through lower startup costs, non-disruptive upgrades and non-impactful redeployments of infrastructure resources, pay-for-use models during the implementation phase, and the flexibility to scale-up resources during intensive development and scale them back down when that development ends.

Enterprise cloud services also provide the highest service levels for availability. Built with redundancy and business continuity by design, a managed EHR platform, when overseen by an enterprise-class cloud provider, can deliver up to 99.999% service level agreements (SLAs) for infrastructure availability, which is less than 6 minutes of unplanned downtime per year. Conversely, an on-premises solution can face limitations in the speed of deployment and scalability and it would be costly to meet comparable business continuity guarantees.

Concerns about the Managed Cloud

Many healthcare providers want to off-load the operations and management of EHR systems because IT resources should be focused on areas that are core to the organization's mission: improving patient care.

While there are many advantages to having a cloud-based service, concerns about losing management control of the EHR technical and functional operations in cloud environments are often a significant factor in a healthcare provider's decision on where to run their EHR system.

Healthcare providers are concerned that the cloud service will lack the processes, methodology and tools that are required to govern a healthcare IT environment, including the EHR platform. There is also concern about managing the communication latency and interfaces between systems when dealing with hybrid deployment, specifically between the applications and EHRs running in the managed cloud environment talking to applications not co-located with the EHR.

In reality, the provider's opportunity when deploying an EHR system in a managed cloud is to work side-by-side with product certified health IT professionals, with deep expertise in infrastructure and security services. Many cloud services, particularly those who support hybrid deployments, offer end-to-end management of the infrastructure and technical components of the EHR applications. The health provider can rely on one group to manage the environments, regardless of where the application runs.

Hybrid is the Way for Healthcare IT

Hybrid architectures for mission-critical, highly connected environments are not new. In fact, it is the most common deployment model. Enterprises regularly leverage combining legacy on-premises environments with the off-premises cloud services. The network between the centers should be a highly secure, completely controlled connection, such as Multiprotocol Label Switching (MPLS) or point-to-point. The cloud environment must also be thoroughly controlled, blending the best practices, procedures and security standards of both the healthcare provider and the partnering cloud company.

Also, the application interdependencies need to be well understood (it's advised to have applications with high data interchange rates or with very low latency requirements in the same location). This means that during the planning and assessment phase of any potential migration it's incredibly important to understand which applications need to stay together and which can tolerate expected latency.

Application interconnection is essential, but the system management is also critical, especially when off-loading portions of previously existing on-premises applications to managed clouds. When moving any part of the healthcare IT landscape, including the EHR systems, to a cloud environment, it's imperative to know who manages the applications and the interfaces that keep data moving smoothly between the separate systems. It's also important to distinguish between the infrastructure operations, the technical management of the applications and the functional management of the applications. It must be well scoped, correctly implemented and managed. When done correctly, the management of the entire healthcare IT landscape can provide the same or better service than an on-premises model, with potentially lower delivery costs.

What to Look for in a Cloud Provider

Healthcare organizations should partner with a cloud service provider that offers a full suite of security and compliance capabilities, guarantees the safety and security of patients' health data, and delivers true "cloud" benefits such as pay-as-you-go, scale-up, scale-down and rapid deployment. Also, make sure there is always someone to call: a 24/7 white-glove service is critical to

keeping healthcare IT systems, including EHRs, running around the clock while compressing costs. A 24/7 service will allow for rapid resolution on any issues that appear within an IT system, dealing with any problems as soon as they become apparent. Lastly, healthcare organizations should search for a cloud provider who will also holistically baseline, monitor and manage the cloud environment to deliver proactive governance and preventative measures to determine potential issues and deal with them before they become a threat.

By choosing a cloud provider who can provide this level of governance and security along with the utility benefits made possible by a large-scale heterogeneous IT environment, a healthcare provider can make a positive impact on their current IT infrastructure while at the same time transforming their systems to be future-ready.

Virtustream EHR Service

Virtustream offers a choice of managed services that can provide healthcare organizations what they need to transform their IT landscape and improve patients' experiences while reducing costs:

- Virtustream Healthcare Cloud with VMware Horizon View: This option is designed for customers that already have the necessary staff or partner resources to manage their EHR application, but require a cloud solution to modernize their business technologies. This option provides managed services for the underlying Virtustream Healthcare Cloud, including management of all infrastructure plus management of the computing platform that serves VMware Horizon View for their published applications.
- Virtustream Healthcare Cloud and Virtustream Managed EHR Platform Service: This option includes managed services for the Virtustream Healthcare Cloud, management of VMware Horizon View for application delivery, and managed services for the EHR platform environment which includes the customer's EHR system database plus the EHR supporting ecosystem.

These choices are designed to complement the EHR application suite management provided by the healthcare provider or their technology partner.

Contact

For more information about Virtustream Healthcare Cloud, please contact us at info@virtustream.com or visit us at www.virtustream.com.

About Virtustream

Virtustream, a Dell Technologies Business, is the enterprise-class cloud service and software provider trusted by enterprises worldwide to migrate and run their mission-critical applications in the cloud. For enterprises, service providers and government agencies, Virtustream's xStream® Management Platform and Infrastructure-as-a-Service (IaaS) meets the security, compliance, performance, efficiency and consumption-based billing requirements of complex production applications in the cloud - whether private, public or hybrid.

