Cloud-based EMR Solutions: Ensuring Reliability, Performance and Security

The healthcare industry is increasingly embracing cloud-based electronic medical record (EMR) systems. Cloud-based EMRs offer scalability and flexibility unmatched by on-premise/installed EMR solutions. Furthermore, cloud-based EMRs offer deployment with low upfront costs and subscription options based on usage (e.g., Software as a Service or SaaS). These attributes make cloud-based EMRs attractive to healthcare providers ranging from large enterprises to small, standalone ambulatory surgery centers (ASCs) to physician practices of any size.

Many healthcare providers, however, still have concerns about cloud-based EMRs. Healthcare providers worry about the reliability, performance and security of cloud-based EMRs as compared to installed/on-premise EMRs. Cloud-based EMR vendors need to be able to address provider concerns in these areas in order to capitalize on the trend toward cloud-based EMR adoption in the healthcare industry.

The importance of reliability

Reliability is an important aspect of any cloud-based application. In healthcare, application reliability is literally a matter of life and death. Providers must be able to access patient information and clinical decision support without interruption, 24/7/365.

For cloud-based EMR vendors, reliability is complicated by the fact that the majority of vendors rely on the internet and public cloud infrastructure as a service (IaaS) for application delivery and hosting. “The internet is not business-ready,” said Greg Lord, senior product marketing manager at Akamai Technologies. “This means users of cloud-based EMRs can have inconsistent experiences, creating provider resistance to adopting cloud-based solutions.

“The reality is that many cloud-based EMR vendors are hosting their applications on public-cloud infrastructure, which they do not own and do not control. Therefore they have no ability to predict downtime or outages, which

Produced by
HIMSS Media

"Many cloud-based EMR vendors are hosting their applications on public-cloud infrastructure, which they do not own and do not control."

Greg Lord
Senior Product Marketing Manager
Akamai Technologies

happen more often than we would like," Lord said. "In healthcare, that means a clinician may not be able to log into that EMR. That's not acceptable."

Performance issues

In addition to concerns about reliability, healthcare providers have concerns about the performance of cloud-based EMRs. "Complaints about EMR performance are one of the things I hear most," said John Daniels, global vice president of the Healthcare Advisory Services Group, HIMSS Analytics. Daniels has visited healthcare providers around the world, on behalf of HIMSS, to assess provider's adoption of EMRs against the HIMSS EMR Adoption Model.

"Physicians and nurses will demonstrate for me how they look up information or access images in the EMR. They click a link, and often we just sit there for a few minutes. Clinicians need the system to be fast and immediate, so they are not wasting their time waiting for a screen to come up when they are face-to-face with a patient," Daniels said. "It's a big concern."

As with reliability, cloud-based EMR performance is generally at the mercy of the internet. Native internet routing and transport protocols can be disrupted and congested by variables as diverse and ever-changing as different geographies coming online as they begin their workday; major cyberattack incidents; or the occurrence of an event such as an election or significant sporting event being broadcast online. All of these and more can cause internet traffic congestion.

"It doesn't matter to the end-user whether the problem is with the internet or the EMR application itself," said Daniels. "If the end-user experiences the EMR as really slow, they will assume something is wrong with the product. Regardless of the cause, slow performance impacts the EMR vendor's reputation."

A seminal study by the Aberdeen Group on the performance of web applications found that a one-second delay in web performance correlated to a 16 percent decrease in customer satisfaction.[1] Decreases in customer satisfaction have consequences throughout the sales cycle for EMR providers. Many prospects for cloud-based EMRs become familiar with the application's features and functionality through online demonstrations. Poor performance of online demo can directly affect sales, since the provider organization will likely not move past the free demo period to become a paying customer.

Once the client has purchased and implemented a cloud-based EMR, performance is even more critical. If the physicians, nurses and other staff who use the EMR are dissatisfied with the application performance, not only can there be negative clinical consequences, but business outcomes will also suffer. Cloud-based EMR solutions are ultimately much easier to replace than on-premise/installed EMR solutions, so providers will not hesitate to switch to a competitor's application. Customer churn can be a direct consequence of poor application performance.

Ensuring reliability and performance for cloud-based EMRs

Cloud-based EMR vendors depend on the internet to deliver applications quickly and reliably. The internet, however, was not designed to provide the degree of reliability and performance required by many service level agreements (SLAs). How, then, do cloud-based EMR vendors ensure reliable, high-quality performance?

"Regardless of the cause, slow performance impacts the EMR vendor's reputation."

John Daniels
Global Vice President, Healthcare Advisory Services
Group HIMSS Analytics

One solution is to partner with a cloud-based application delivery platform to facilitate application delivery. Cloud-based application delivery platforms leverage the benefits of using the internet (e.g., accessibility and global reach) and at the same time, employ strategies to overcome the internet's inherent weaknesses. "Cloud-based application delivery platforms connect the application to the end-user to optimize end-to-end delivery, ensuring a great experience for all users – regardless of where they are located or the device they are using," said Lord.

The most effective cloud-based application delivery platforms comprise hundreds of thousands of servers and thousands of networks. This provides many critical advantages for cloud-based application delivery. Servers are strategically deployed to ensure proximity to cloud data centers where applications are hosted, as well as proximity to end-users. Because cloud-based EMR applications are highly dynamic, a highly distributed application delivery platform is required to ensure the end-to-end optimization of the internet connection between the application and the end-user throughout the entire session.

In addition to leveraging the physical proximity of the platform to ensure reliability and performance, cloud-based application delivery platforms also employ intelligent logic and design. For example, cloud-based application delivery platforms monitor the constantly changing internet conditions and evaluate the fastest route for each user at each point in time. Instead of defaulting to native internet routing and peering protocols, the application delivery platform employs its own logic and intelligence to select the fastest internet route between the user and the application.

"Effective application delivery platforms detect where the user is, what network connectivity they have and what device is being used to access the internet. The platform is able to optimize for all of these variables in real-time to ensure the best possible user experience," said Lord.

Security concerns

Data security is also a top concern for healthcare providers. "Clinical data is highly valuable. It is worth more than credit card data on the black market," said John P. Hoyt, executive vice president emeritus of HIMSS Analytics. "That is one reason why privacy and security are extremely important." Healthcare providers who violate the privacy and security requirements defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) risk incurring federal and state penalties and fees, damage to the organization's brand and the possibility of class action lawsuits.

A healthcare provider's internal policies, procedures and practices play a significant role in ensuring the security of protected health information (PHI). The addition of a cloud-based component to the management, transmission and storage of PHI introduces an element of uncertainty for providers. "If you are choosing a solution that is being hosted somewhere other than your own facility, you have to be convinced of the credibility of the hosting organization to provide that security," said Hoyt.

The requirements for privacy and security apply not only to remote data centers, but also to the transmission of data between remote data centers and the end-user. Default internet security protocols are not generally considered to be adequate for providing the level of security required for PHI.

"If you are choosing a solution that is being hosted somewhere other than your own facility, you have to be convinced of the credibility of the hosting organization to provide that security."

John P. Hoyt
Executive Vice President Emeritus
HIMSS Analytics

Ensuring security for cloud-based EMRs

In the same way that cloud-based application delivery platforms enhance application performance and reliability, these platforms can also improve the privacy and security of information traveling over the internet. As noted earlier, effective application delivery platforms comprise hundreds of thousands of servers. The same servers, deployed at the "edge" of the internet, provide a means of keeping malicious cyberattacks at bay, far from either the healthcare provider's data center or the application provider's data center. The most effective cloud-based application delivery platforms have the scale to absorb large cyberattacks without affecting application performance.

As Hoyt pointed out, being able to provide both reliability and security in an EMR system, without one cancelling out the other, is important. "You could have a super secure system that is unreliable – and people would hate it because of possible access requirements. You could have a highly reliable system that is not secure, and the users would not even know it. You have to have a reasonable balance," said Hoyt.

Achieving quality, safety and efficiency with cloud-based EMRs

EMRs – whether cloud-based or on-premise – are ultimately employed to advance quality, safety and efficiency within the healthcare industry. Cloud-based EMRs hold the potential to advance these three aims by providing scalable, flexible, cost-effective EMR solutions. However, vendors must find ways to address issues of reliability, performance and security in order to ensure broader acceptance of cloud-based EMR solutions. Collaborating with a cloud-based application delivery platform can be an effective approach to addressing provider concerns about reliability, performance and security – and gaining the trust of healthcare providers.

[1] Aberdeen Group. (2008, Nov. 30). "The Performance of Web Applications: Customers are Won or Lost in One Second."

Produced by HIMSS Media | www.himssmedia.com | © 2016