Cloud Computing and Healthcare Security: 4 Things to Track

Amanda Herriman, Marketing Manager

Healthcare Marketing

April 5, 2019

As cloud computing becomes the storage option of choice for the healthcare industry, the issue of security is an increasing concern for institutions. With an average of nearly 32,000 intrusion attacks *per organization per day* in 2017 (compared with 14,300 for other industries) healthcare is, to quote, "in a world of cybersecurity hurt."

That doesn't mean it's not in your best interest to adopt cloud computing—just that you have to take extra care to track the following four critical issues when you're selecting an option.

#1: Data Security

No surprise this one is top of the list, given the value of data. Every healthcare data breach averages $380 per record. That's more than double the value of the average data breach in other industries. Many data centers and cloud computing companies are actively looking at ways to protect healthcare data, so be sure to choose a provider who specializes in cloud architectures developed to protect data and meet HIPAA compliance requirements.

#2: Total Ownership Cost

It's not rocket science, but it could cost as much! Cloud computing can be expensive, particularly if it isn't properly designed. Many healthcare organizations learned this lesson the hard way in the beginning, but cloud design has matured now and providers can usually determine the usage, data requirements and workloads during the early stage of a cloud project.

Focus on granularly identifying the data points, workloads, and users that need to live in the cloud ecosystem to get the best possible pricing, then plan ahead for where you'll need more resources for future deployments. Almost any system can be made totally reliable (like NASA), but the cost could be too high.

#3: Network Reliability and Performance

There's no point in having patient records in the cloud if the system is down when you need lifesaving information. This makes system reliability vital to cloud entry for healthcare organizations. With the rise of telemedicine and the Internet of Things (IoT) bringing more connected devices almost daily, cloud networks absolutely cannot afford any latency or poor performance risks in their design.

Data and applications could be essential to saving lives, delivering critical services and avoiding medication errors, so organizations making a shift to the cloud need to track this aspect closely.

#4: Service Level Agreements (SLAs)

Few healthcare organizations are likely to risk entering a vendor relationship without a comprehensive SLA in place, and cloud computing is no exception. This sets expectations for all parties and acts as a roadmap for navigating both anticipated changes and unexpected events. Some of the criteria your SLA should cover includes:

- system availability
- performance
- security
- disaster recovery expectations
- data location/compliance with local legislation
- accessibility and portability
- change management process
- dispute mediation guidelines
- exit strategy

Other issues surrounding cloud computing and healthcare security that require careful attention are the challenges associated with migration, data ownership, and the skills required by employees to handle the change. Working with a good service provider can help you realize a smooth transition and deliver excellent healthcare security for your stakeholders.

To learn more about cloud computing and healthcare data security, call Wax Custom Communications at 305-350-5700 or visit waxcom.com.