Who's responsible for protecting patient data in the cloud?

Cybersecurity experts lay out the facts, and misperceptions, about securing data in the cloud. The answer is not so simple.

By Bill Siwicki
July 18, 2017
04:42 PM

Cloud computing is still fairly new to healthcare and, as such, confusion and a few myths surround the technology. And many of those skewed perceptions are driven by simple misunderstandings, most notably about information security.

Indeed, cloud providers offer a lineup of advantages that on-premise solutions sometimes do not: physical and software security, access control for authentication, regulatory compliance, advanced encryption, high availability and data center redundancy, continuous monitoring, as well as multi-tenant segmentation.

And there’s evidence that a major shift to cloud services is underway for security and other applications.

“People believe that the companies who invest their focus on a particular service or application bring next-level, dedicated expertise to securing that application, certainly more than any IT shop would,” said Bill Ho, CEO of Biscom.
Cloud security puzzle
Many cloud providers offer the tools and integration points for customers to secure their
apps and data with advanced protections to prevent breaches and data loss. But that is
only half of the security puzzle. The other half is a hospital’s responsibility to secure its
own data assets.

Put all those pieces together and it appears to form a safe and secure place for
protected health information and personally identifiable information, right?

Not so fast.

“Data isolation does not protect against malware or advanced threats,” said Krishnan
Subramanian, product marketing manager at Check Point Software Technologies.

As more and more hospitals turn to cloud services, in fact, it is becoming critical for IT
and security teams to understand that delineation of cybersecurity responsibility.

Cloud security a joint effort
A Biscom survey of 631 U.S. full-time employees in various industries, including
healthcare, who are active users of cloud services at work, found more than half report
their overall concerns about cloud security have dropped during the past five years.

“Much like swimming in the ocean alone or with others, the number of sharks remains
the same – but with a large group, you feel safer and almost supported,” Ho said. “While
not necessarily true, the abundance of cloud offerings have made the idea of using the
cloud far less dangerous than originally thought.”

That’s not to say hospital security professionals and staff do not recognize dangers
lurking in the cloud, however, as 62 percent of participants in Biscom’s research said
they believe major security gaps exist in the cloud services they use at work.

All of which brings health IT executives and infosec pros back to the original question of
who is ultimately responsible for protecting PHI and PII when it resides in the cloud?

“It’s the shared responsibility model where both cloud provider and customer have a
role to play,” Check Point’s Subramanian said.

Cybersecurity, in other words, is a joint effort and each party brings critical security
controls to the table that complement each other to piece together comprehensive
protection of data in the cloud, Subramanian added.