How Secure is the Healthcare Cloud?

Security of patient data is a key aspect of a hospital's operation. Thus, it's important for healthcare providers to ensure that they only deal with IT companies that can develop solutions that are secure and won't compromise patient records.

Amidst rising incidents of cybercrime, hospitals should heed this warning from a healthcare IT expert: that many cloud computing vendors lack the ability to appropriately secure health data. The warning was issued by John Houston, vice president of security and privacy and associate counsel at University of Pittsburgh Medical Center (UPMC).

"When evaluating a vendor, we find that they just simply don't have the wherewithal, the ability to develop a solution that is in fact appropriately secure," says Houston.

When security professionals at UPMC were evaluating a cloud services vendor, they managed to circumvent a particular vendor's security. They reported this to the cloud provider who said "no you haven't". UPMC's IT team gave the vendor a customer's data back, proving their point.

However, the same thing happened on a second test and even a third.

"After the third time of not being able to secure their application they finally said, 'listen, we're a small company, we only have three developers and they don't really understand security,'" Houston says, noting that such kind of revelation is not limited to small cloud companies.

See Also: **Cloud Computing for First Responders**

According to Houston, he has encountered several situations in which a company looked very credible and seemed to have its act together.

"But behind the scene they really don't," he points out. "When evaluating a vendor, we find that they just simply don't have the wherewithal, the ability to develop a solution that is in fact appropriately secure."

Similar to other large institutions, UPMC spends considerable chunks of time and effort to really secure its data. What Houston wants to happen is for vendors to be more transparent about their security offerings and to support standards such as HITRUST, the Health Information Trust Alliance.

HITRUST implements the Common Security Framework certification, which is aimed at reducing cyber threats and cybercrimes.

"My attitude is that vendors ought to do the same thing. I should be able to go to them and say where's your latest HITRUST assessment and your latest HITRUST score?" says Houston. "And they should be able to give that to me."

Published on : Mon, 5 Dec 2016