HealthManagement.org
Promoting Management and Leadership

Top Healthcare Cloud Security Concerns

In spite of security concerns with the healthcare cloud, the sector continues to increase its adoption of this technology.

HealthITSecurity.com, has recently examined the cloud saying that while many covered entity organisations are not considering its use in the immediate future, understanding top present and potential security concerns is important for as smooth a security operation as possible following any implementation of the technology.

In an effort to understand the cloud, *HealthITSecurity.com* explains the three main types of storage.

1. Software as a service (SaaS). This "is where the cloud service provider provides access to certain software functions, such as word processing or email. The cloud service provider will also cover any software upgrades or maintenance issues."

2. Platform as a service (PaaS), "where customers might have remotely accessible computing power and can run some of their own applications. However, they are still not required to handle their own maintenance."

3. Infrastructure as a service (IaaS). "In this scenario, customers might have remotely accessible computing power, will be able to run some of their own applications, and will be charged with handling any maintenance issues."

The cloud in healthcare can be very beneficial, says the report, including allowing covered entities to store information off-site. Furthermore, remote or mobile employees can still access important information.

Another advantage of the cloud is organisations can reduce operating or storage costs releasing resources for maintaining software, platforms, or infrastructure.

In considering using the cloud, it is critical to remember that the HIPAA Omnibus Rule needs patient data to be protected, regardless of its storage location. "Companies that are working as a third-party firm, and do not necessarily review the data on a regular basis, must still adhere to HIPAA regulations."

The report goes on to say that one of the top healthcare cloud security concerns is the compromise of sensitive information, such as PHI.

Security experts have found that excessive PHI sharing is a key concern for healthcare organisations using cloud security. Other areas of concern included diagnosis, financial information, medical condition, and Social Security numbers.

Owing to federal security criteria, the rate of cloud adoption rate has increased more swiftly in unregulated industries than in healthcare in recent years.

With hacking one of the most routine security breaches in IT healthcare, as with all technology applications, health bodies need to carefully examine how the cloud works in order to implement better security measures.

Source: Health It Security

Image Credit: Pixabay

Published on : Mon, 23 May 2016