Security in The Cloud

How to evaluate the data security capabilities of cloud-based services

By Cristine Kao, Global Manager, Healthcare Information Solutions, Carestream Health

As many healthcare systems consider the advantages of moving patient data to a cloud-based service, radiology and IT managers are understandably concerned about data security. The good news is that healthcare facilities of all sizes can achieve more comprehensive data security from healthcare cloud service suppliers due to their expertise and investment in advanced technologies, infrastructures and processes.

If you are considering cloud services, it's important to evaluate each supplier's ability to deliver all three components of data security: availability, integrity and privacy. Data availability delivers continuous access to data even in the event of a natural or man-made disaster or event, such as fires or power outages. Data integrity ensures that the data is maintained in its original state and has not been intentionally or accidentally altered. And privacy refers to successfully restricting access to authorized persons.

To maintain continuous security in the cloud, all three forms of data security should be maintained within the physical infrastructure of the supplier's data center, the hosted application that manages data and the policies and procedures.

Ensuring availability involves physical security features, such as redundant power supply and air conditioning systems, protection against fire and specially equipped ventilating and air conditioning systems. The cloud services provider should maintain at least two copies of ingested data, thus reducing the risk of data loss. The second copy, active or passively synchronized, should be stored at another location in case a disaster impacts the primary data center. Databases and data must be stored on architectures that provide high availability and performance.

Data Security and Integrity

This is a key area where cloud services excel. Access to the data center must be

Cloud Storage Providers

A comparison chart featuring providers of cloud storage appeared in the March 2012 issue of *ITN* and is archived online at itnonline.com. To find information from 18 vendors, visit www.itnonline.com/comparison-charts?t=Cloud+Storage+Systems or scan this QR code on a smartphone.

tightly monitored through the use of security guards, a scheduling process for any visitors, a single entrance to the most sensitive area of the data center, and surveillance cameras around the building and at each entrance. Employee access should be monitored, and extra authentication should be required to access sensitive areas within the building where patient data is stored. You should also ask to see the supplier's security policy and find out how employees' online access to data is monitored.

Data integrity involves a validation process to ensure each copy of the data maintains its integrity. Damaged files must be able to be detected and reconstructed. Application-level signatures should be computed for every document and kept in the database. The encryption mechanism used to ensure the confidentiality during the transmission includes an integrity check that prevents the risk of data corruption during its transmission over TCP/IP.

The key used to encrypt the data should be encrypted with the data itself. If data has been modified intentionally, or accidentally, data decryption would then fail. This protection also prevents the sending of corrupted data to clinicians and other users.

Ensuring Privacy

Privacy protection is required at both the application and network level. Communication between healthcare sites and the data center is performed with SSL-based encryption at the application level to ensure end-to-end protection between the service access point and the data center. This encryption ensures that none of the employees of the network provider can access data and prevents data from being viewed while it is being carried over the Internet to an end user's viewing software.

SSL can implement several encryption algorithms. Site-level access control defines which originating sites can access data, and a user profile defines access to features and data. Access rights for a given user can be defined for patients and types of studies. Secure access requires each data center to equip its Internet connection with the following:

- Firewalls to control network transmissions based on a set of rules that protect networks from unauthorized access;
- a physical or logical subnetwork (known as a demilitarized zone) that contains and exposes an organization's external services to a larger untrusted network, providing security from external attacks; and
- permanent updates to anti-virus software with the latest virus signature databases.

To guarantee secure data exchange, the connection between the data center and a customer site is usually made through an SSL-encrypted tunnel.

Policies and Procedures

Beyond physical and application level design, proper policies and procedures are required to maintain ongoing security for cloud-based services. These involve establishing an audit trail that tracks all patient health information (PHI)-related activities, warnings and failures that occur in the system. This information can be used to trace the source of selected changes to information in the system, as well as to detect unusual system activity.

Proactive monitoring combines technology with experienced personnel to enable early detection of potential incidents, ideally before they impact users. A dedicated tool permanently watches each node of the cloud infrastructure, along with access points at each customer's location and platforms at data centers. Monitoring controls key application processes, systems and wide area network between the service access point and the data center.

A remote monitoring system infrastructure collects metrics from each device and automatically triggers alerts when a faulty condition is detected. Conditions that trigger an alert range from data that is not being backed up to unauthorized attempts to access data. Depending on the severity of the incident detected, an e-mail may be sent to the support team or a visible alarm may be displayed at the dashboard to initiate follow-up action.

In addition to protecting data, monitoring activities also ensure that the systems achieve specified performance and uptime guarantees. Monitoring is conducted 24/7/365, and trained personnel investigate each incident.

It's often cost-prohibitive for individual healthcare systems to invest and provide ongoing support for equipment, technology, personnel and training that's required to deliver the highest level of data security across all physical locations and communication methods. Providers may want to consider working with a cloud services provider that can provide a higher level of data protection. itn