Technical Brief Series

How to Evaluate the Data Security Capabilities of Cloud-Based Services

Executive Summary

One of the critical issues in evaluating cloud-based services is data security. Cloud-based services today can be compared to Internet banking. Consumers were initially afraid that online banking would make them more vulnerable to fraud or identity theft. Now that online security technologies have improved, online banking is actually safer than getting paper statements in the mail.

Likewise, using a cloud-based service supplier can be a major step toward preventing serious security issues. However, you must choose your provider wisely. Suppliers must demonstrate that they have the optimal technologies, infrastructures and processes in place to ensure data security. And healthcare providers need to require evidence that health information is protected at all levels and stages of the workflow – from duplicate disaster recovery copies and physical protection of the data center to data transmission, storage, and user access.

It's important to understand the four key components of data security: availability, integrity, confidentiality, and traceability.

Availability ensures continuous access to data even in the event of a natural or man-made disaster or events such as fires or power outages. **Integrity** ensures that the data is maintained in its original state and has not been intentionally or accidentally altered. **Confidentiality** means information is available or disclosed only to authorized individuals, entities, or IT processes. And **traceability** is the ability to verify the history, location, or application of an item by means of records.

All components of data security must be maintained at the following three levels:

1. The physical infrastructure of the data center;
2. The hosted application that manages data; and
3. The policies and procedures to maintain continuous security in the cloud.

1. Physical Security at the Data Center

The data center must supply a secure physical hosting environment. This typically includes:

- Redundant utilities, particularly power supply and air conditioning.
- Protection against fire with appropriate extinguishers in each computer room, as well as emergency power-off switches.
- Specially equipped ventilating and air conditioning systems.
- Windowless rooms for servers and storage equipments.
- Access control to enter the data center. This includes access monitoring through badge-based entry, security guard at the building entrance, no unscheduled visits, a single entrance to the most sensitive area of the data center, and surveillance cameras around the building and at each entrance. Ask to see the supplier's security policy and find out how employees' online access to data is monitored.

The Uptime Institute classifies data center designs into four tiers. Most hospital data centers are a Tier 1 or Tier 2. Typically, cloud service providers are Tier 3 and Tier 4 because they are best equipped to make the significant investments required to guarantee higher security.

Tier Level	Requirements
1	• Single path for power and cooling distribution • Non-redundant capacity components (single uplink and servers) • 99.671% availability
2	• Single path for power and cooling distribution • Redundant capacity components • 99.741% availability
3	• Multiple active power and cooling distribution paths, but only one path active • Redundant capacity components (dual-powered equipments and multiple uplinks) • Concurrently maintainable site infrastructure • 99.982% availability
4	• Multiple active power and cooling distribution paths • Redundant capacity components • All components are fault tolerant, including chillers and heating, ventilating and air-conditioning (HVAC) systems • 99.995% availability

2. Application-Level Security Design

Application-Level Availability

Any application should start with a secure and reliable storage mechanism:

- The cloud service provider should maintain at least two copies of ingested data, thus reducing the risk of data loss. One of the two copies is made on removable media so it can be stored at another location—in case a disaster impacts the data center. The system should ensure that the two copies are permanently synchronized.

- Database is stored on RAID-10 (1+0) disk system. RAID-10 provides a high level of fault tolerance and adequate performance for small random IOs.

- Data is stored on RAID-6.
RAID-6 provides an excellent level of fault tolerance, with a higher ratio of usable/physical storage and the right performance for large sequential IOs.

Application-Level Integrity

It is not enough to maintain and keep available two copies of patient data, the cloud service provider must also have a validation process that ensures that each copy of the data maintains its integrity. Responsibility for maintaining data integrity should be clearly defined as part of any contract with a service provider.

Multi-Level Data Confidentiality

Cloud-based services suppliers must be committed to respecting privacy and protecting PHI. Compliance to Health Insurance Portability and Accountability Act (HIPAA), the European Union's Data Privacy Directive and other local regulations is mandatory.

Data protection is required at both the application and network level. Communication between healthcare sites and the data center is performed through an SSL-encrypted tunnel 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. It also prevents data from being viewed while it is being carried over the Internet to an end user's viewing software.

Carestream Health, Inc., 2012. CARESTREAM is a trademark of Carestream Health. 7185 ENT FQ 0212

In healthcare environments, access control must also combine with minimally two levels of privilege authentication:

- Site-level access control defines which originating sites can access data. By default, data ingested by an originating site shall only be accessed by users from the same site. Any other access, such as queries from other sites or from the web portal, must be specifically set up.
- A user profile specifies access to both features and data. Access rights for a given user can also be defined for patients and types of studies.

Secure Connection to the Cloud

Secure access requires the data center to equip its Internet connection with the following:

- Firewalls to protect networks from unauthorized access and attacks.
- Demilitarized Zone (DMZ), a subnetwork that contains and exposes external services to Internet, providing additional security from external attacks.
- Permanent updates to anti-virus software with the latest virus signature databases.
- Intrusion Detection Systems (IDS) to report malicious activities on networks and systems.

3. Policies and Procedures to Maintain Security

Beyond physical and application-level design, proper policies and procedures are required to maintain on-going security for cloud-based services, completing the traceability component of the security design.

Establishing an Audit Trail

While data privacy addresses who can access data and what a user can do, a comprehensive auditing function is needed to track all PHI-related activities, warnings, and failures that occur in the system. This audit information can be used by security administrators to trace the source of selected changes to information in the system, as well as to detect unusual system activity.

Remote, Proactive Monitoring

Remote, proactive monitoring is an extremely important function offered by leading cloud-based services, requiring both technology and experienced personnel. Monitoring enables early detection of potential incidents, ideally before they impact users.

Monitoring is executed by a dedicated tool that permanently watches each node of the cloud infrastructure, along with access points at each customer's location. Monitoring controls key application processes, systems, and wide area network between the service access point and the data center.

An appropriate proactive monitoring infrastructure collects metrics from each device and automatically triggers alerts when a faulty condition is detected. It is important that monitoring is conducted 24/7/365 and trained personnel investigate each incident.

In addition to protecting data, monitoring activities also ensure that the systems achieve specified performance and uptime guarantees.

Defining the Appropriate Security Policy

The final element in a comprehensive security system is the organization's Security Policy. The Security Policy tracks how security is achieved through the various technical and human resources aspects of the product, operations, and organization. It also provides a risk assessment. The Security Policy is maintained under the responsibility of a designated Security Officer.

The Security Policy addresses the following topics:

- Organization: It defines the boundaries of responsibility of all involved stakeholders. For instance, upgrades and monitoring shall be performed by operations, while software engineering is the only department that has access to source code.
- Enforcement and follow-up of Security Policy: The Security Officer maintains the Security Policy and ensures that it is applied. Internal audits are conducted and corrective actions are identified and implemented.

Carestream Health, Inc., 2012. CARESTREAM is a trademark of Carestream Health. 7185 ENT FQ 0212

- Risk assessment: It identifies possible threats, vulnerabilities and countermeasures. This assessment is regularly updated.

- Human resources: The Security Policy lists security procedures to be used when employees are hired, resign, or move within the organization.

- Physical security: The data center should restrict physical access and require badges to enter specific areas. Security guards protect the removal of equipment and prevent any unauthorized access.

- Network security: It shows how networks are protected from intrusions, attacks, unauthorized access or illegal tapping. VPNs and firewalls are the usual technologies in this area.

- Server security: It describes how servers are hardened and protected. It shall include the anti-virus policy.

- Business continuity: It refers to those activities performed daily to maintain service, consistency, and recoverability. It includes a description on how fault tolerance and disaster recovery are ensured.

- Access control: It lists how and from where sensitive data can be accessed and restricts access to appropriate users with authentication systems.

- Data protection: Typically, it describes the data lifecycle management (number of copies, locations of these copies, conditions for data destruction, etc.) and the procedures to ensure that PHI is secured.

- Traceability: It ensures that every critical operation, such as access to PHI, is logged and audited.

- Security incident management: It describes the tracking and logging of all security incidents.

- Compliance: It states how the Security Policy ensures that all local regulations are respected and that required certifications are reached.

Every healthcare organization needs to ensure that the security policy is endorsed and implemented as part of each element in a cloud–based operation.

Conduct a Background Check on Suppliers

Many cloud-based services vendors make the same claims, so how can a healthcare provider decide which supplier offers a better solution? In addition to evaluating data security techniques, conduct a background check on the cloud services provider. How long have they maintained cloud-based services? Ask for customer references.

Carestream Health is a well-respected, worldwide cloud-based services provider that manages 30 million studies (1 Petabyte of data) in ten different clouds. Carestream is a world leader in the technologies, infrastructures, and processes that deliver healthcare data security and privacy. Health information is protected at all levels of the workflow—including the physical infrastructure of the data center, the hosted application that manages data, and the policies and procedures to maintain continuous security in the cloud.

CARESTREAM Vue for Cloud Services

Conclusion: Cloud-Based Services Can Provide the Highest Level of Data Security

It is cost-prohibitive for most individual healthcare providers to support the investment in the equipment, technology, personnel, and ongoing training required to deliver the highest level of data security. Converting to best-in-class cloud-based services allows healthcare providers to achieve industry-leading data security—including data availability, integrity, confidentiality, and traceability. This security is delivered through the physical infrastructure of the data center, the hosted application that manages data, and the policies and procedures that govern data access, audit trails, remote monitoring, incident management, and business continuity.

As the standards for data security rise, it's time to evaluate cloud-based services from a world-class provider. Selecting the best cloud-based services provider for your needs allows this technology to liberate you from security problems.

Carestream Health, Inc., 2012. CARESTREAM is a trademark of Carestream Health.