Technical Brief Series

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

Executive Summary

When evaluating cloud-based services, no issue is more critical than 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. But as online security technologies and processes have improved, online banking is now actually safer than getting paper statements in the mail.

Likewise, using a cloud-based service supplier instead of operating your own internal system can be a major step toward becoming liberated from 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 the security of your data. And each healthcare facility needs 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. **Traceability** is the ability to verify the history, location or application of an item by means of documented recorded identification.

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.
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. While temperature is an important factor, equipment must also be protected from external heavy pollution such as smoke from a nearby fire.
- Windowless rooms for servers and storage equipment.
- Access control to enter the data center. This includes access monitoring through methods such as badge-based entry in tandem with a security guard or biometric identification system, strictly controlled visits, a single entrance to the most sensitive area of the data center, and surveillance cameras around the building and at each entrance. Extra authentication should be required to access sensitive areas where patient data is stored. Ask to see the supplier's security policy and find out how employees' online access to data is monitored.

Data center designs can be broken down into four tiers. Most hospital data centers are at Tier 1 or Tier 2. For Tier 3 and Tier 4, cloud service providers are best equipped to make the significant investment required to guarantee higher security.

Tier Level	Requirements
1	• Single non-redundant distribution path serving the IT equipment • Non-redundant capacity components • Basic site infrastructure that guarantees 99.671% availability
2	• Fulfills all Tier 1 requirements • Redundant site infrastructure capacity components that guarantee 99.741% availability
3	• Fulfills all Tier 1 and Tier 2 requirements • Multiple independent distribution paths serving the IT equipment • All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture • Concurrently maintainable site infrastructure that guarantees 99.982% availability
4	• Fulfills all Tier 1, Tier 2 and Tier 3 requirements • All cooling equipment is independently dual-powered, including chillers and heating, ventilating and air-conditioning (HVAC) systems • Fault-tolerant site infrastructure with electrical power storage and distribution facilities that guarantee 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 maintains at least two copies of ingested data, thus reducing the risk of data loss. One of the two copies should reside in a backup data center at a separate location in case a disaster impacts the main 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 high availability and performance when there is a need to reconstruct data in the case of disk failure.
- Data is stored on RAID-6. While this type of RAID is slower to reconstruct in case of disk failure, it offers excellent reliability with a higher ratio of usable storage to physical storage.

One of the often-overlooked areas of data security is authentication procedures. It is not enough to maintain two copies of patient data. The cloud service provider must also have a validation process to ensure that each copy of the data maintains its integrity and that any damaged files can be quickly detected and reconstructed from a RAID copy.

Application-Level Integrity

Application-level signatures should be computed for every document and kept in the database. The encryption mechanism used to ensure confidentiality during the TCP/IP transmission includes an integrity check that prevents the risk of data corruption.

The Transport Layer Security (TLS) protocol and its predecessor Secure Socket Layer (SSL) provide for privacy and data integrity in communications between two computer applications. When secured by TLS, connections between a client and server (such as the connection between a web browser and a cloud-based application) have one or more of the following properties:

- The connection is private because symmetric cryptography is used to encrypt the data transmitted. The keys for this symmetric encryption are generated uniquely for each connection and are based on a shared secret negotiated at the start of the session. The server and client negotiate the details of which encryption algorithm and cryptographic keys to use before the first byte of data is transmitted. The negotiation of a shared secret is both secure and reliable.
- The identity of the communicating parties can be authenticated using public-key cryptography.
- The connection is reliable because each message transmitted includes a message integrity check using a message authentication code to prevent undetected loss or alteration of the data during transmission.

Multi-Level Data Confidentiality

Data protection is required at both the application and network level. Communication between healthcare sites and the data center is performed with TSL/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. It also prevents data from being viewed while it is being carried over the internet to an end user's viewing software. TSL/SSL can implement several encryption algorithms, the most common being AES, 128-bit key length encryption.

Access control also combines two levels of restriction:

- Site-level access control defines which originating sites can access data. A default configuration specifies that data ingested by an originating site may only be accessed by the same site. Patient data can be shared between health establishments, such as a regional healthcare organization, providing that the service has been enabled under formal agreements and specific access controls are in place. Any other access, such as queries from other sites or from the web portal, must be specifically set up. This restriction applies to most imaging IT clouds that require a local server as a point of access.

- 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 control network transmissions based on a set of rules that protect networks from unauthorized access.

- A demilitarized zone (DMZ), which is a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, providing security from external attacks.

- Permanent updates to antivirus 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 a TSL/SSL-encrypted tunnel.

3. Policies and Procedures to Maintain Security

Beyond physical and application-level design, proper policies and procedures are required to maintain ongoing 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 activities, warnings and failures related to patient health information (PHI) that occur in the system.

A trusted cloud service provider should provide robust data that can be used for auditing and other system performance tools, supporting the security administrator in managing the system.

Remote, Proactive Monitoring

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

Monitoring should be executed by a dedicated tool that 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 the 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 fault condition is detected. Conditions that trigger an alert can range from a failure to back up data to unauthorized attempts to access data. Depending on the severity of the incident detected, the monitoring system might send an email to the support team or open a case file and display a visible alarm at the dashboard, allowing follow-up action to be performed by the incident-management team.

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

Defining the Appropriate Security Policy

The final element in a comprehensive security system is the organization's security policy and its support team. The security policy tracks how security is achieved through the technical and human resources aspects of the product, operations and organization.

The security policy is maintained under the responsibility of a designated security officer. The security officer must be involved every time a change is performed to the infrastructure or to the services that could impact data integrity or confidentiality. This includes upgrades, new functionality or organizational changes.

The security policy should address the following topics:

- **Security organization:** The security officer ensures that the security policy is updated. Internal audits are conducted and corrective actions are identified and implemented.
- **Human resources:** The policy lists security procedures to be used when employees are hired, resign, or move within the organization. Forms must be signed by employees, and security training must be conducted. When an employee leaves, specific network access must be disabled and equipment such as tokens must be returned.
- **Assets management:** This section of the policy outlines procedures to ensure that patient information is identified and well-managed. It describes how data must be destroyed when required. It explains how equipment is identified (serial number, internal identification number) and where this information is stored and maintained.
- **Physical security:** Data center security is the responsibility of the hosting company, but the list of employees allowed to enter the data center is maintained internally and communicated to the hosting company. The data center should restrict physical access and require badges to enter specific areas. Security guards prevent the removal of equipment and any unauthorized physical access.
- **Operations:** This section defines the boundaries of responsibility of the hosting company, operations and R&D. For example, upgrades and monitoring should be performed by operations, while R&D is the only department with access to source code. The policy should describe which technical solutions are in place, and enumerate the protocol and encryption mechanisms to be used from the customer site to the data center resources. The policy should also describe how data is secured (replication, media, etc.), how changes are tracked (logs) and methods for database backup.
- **Access control:** The policy should list how and from where sensitive data can be accessed, and restrict access to appropriate users using Secure Remote Service Access (SRSA), secure ID, authentication with login and passwords. It should also describe how servers are hardened and protected.
- **Security incident management:** This section describes the tracking and logging of all security incidents. Depending on incident severity, the security officer may coordinate immediate corrective action and communicate with R&D (to develop a workaround), operations (to deploy), human resources (should the incident involve an employee) and the legal department (in case of a regulation or contract violation).

- **Business continuity:** This section of the policy describes the technical solutions – such as RAID, cluster, network and fiber redundancy – that ensure continuity in the event of a disruptive incident.

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

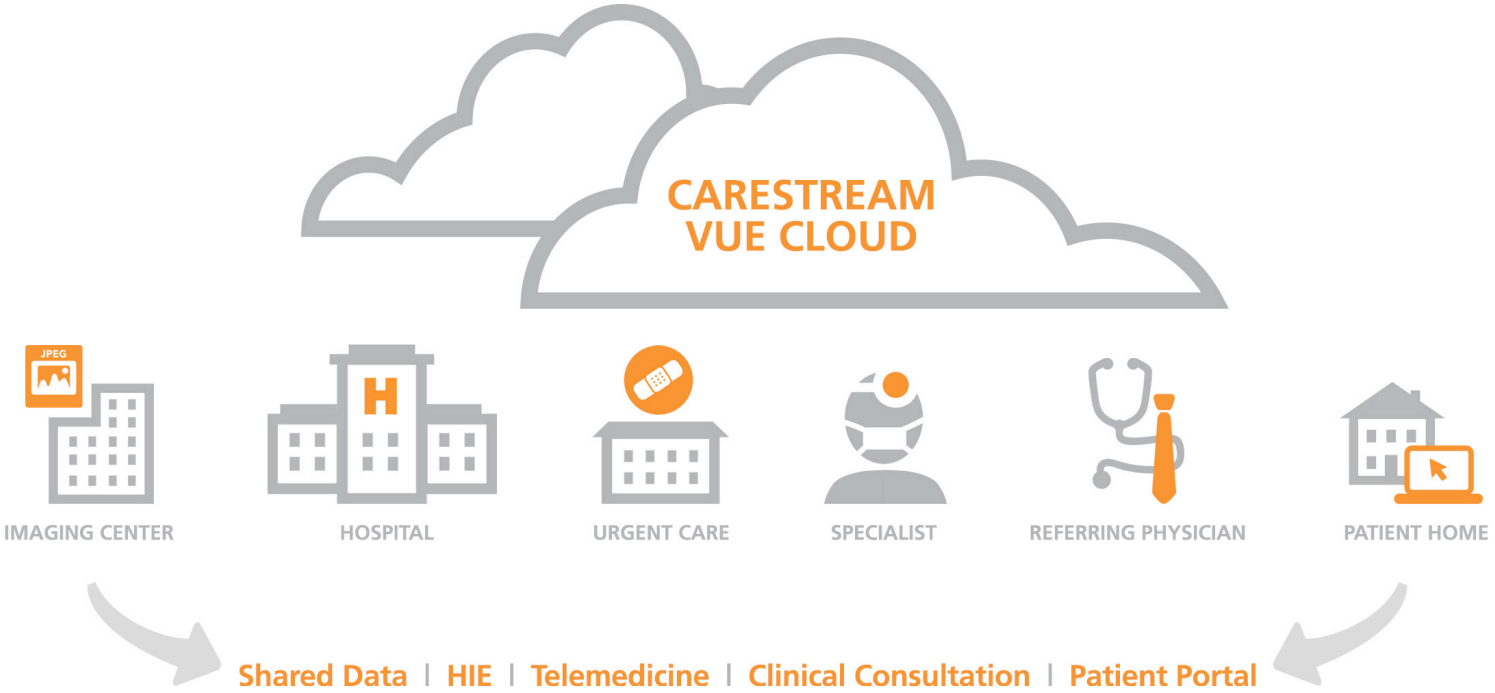
Check the Security Supplier's Credentials

When a healthcare enterprise purchases a PACS or archiving system, it is purchasing features that the user must support and protect. Purchasers of cloud-based services are investing in a high-quality service that includes not only uptime guarantees but also data security levels. Security certification provides assurance that the provider adheres to the industry's best practices for data security.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) have created a standard for information security management: ISO/IEC 27001. The most trustworthy providers of hosted security services have been audited by a third-party accredited certification body and have been granted a certificate of compliance with this standard.

Carestream Health's cloud business in Europe has been certified by BSI Group (also known as the British Standards Institution) as meeting the requirements of the latest published standard, ISO/IEC 27001:2013. This certification means that BSI auditors have examined and approved of all our security processes and controls at every site, and have determined them to be in full compliance with the standard. Certification also requires a yearly surveillance audit. The certificate is valid for three years, after which the full certification process must be repeated.

.



Carestream Delivers Secure Cloud-Based Collaboration for More Efficient, Effective Care

It is cost-prohibitive for many individual healthcare systems to support investments 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.

Carestream Health is a worldwide provider of cloud-based healthcare IT services, offering state-of-the-art technologies, infrastructures and processes to ensure healthcare data security and privacy.

We currently manage 13 private and public data centers with over 12 petabytes of data replicated between multiple sites for backup, disaster recovery and business continuity. We protect health information 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 that govern data access, audit trails, remote monitoring, incident management and business continuity. Our ISO/IEC 27001:2013 certification is a stamp of approval from the world's foremost standards and certification bodies.

Our flagship Clinical Collaboration Platform is designed to bring patient-centric diagnostic imaging to stakeholders across the healthcare enterprise. With anywhere/anytime image access and management – based on a unified core with extensible modules for enterprise-wide integration – it's the ideal application for the cloud. Carestream's Vue cloud services enhance the Clinical Collaboration Platform with:

- Security that provides the highest levels of availability, integrity, confidentiality and traceability.
- Protection against obsolescence, with no need to upgrade hardware and software over time.
- Predictable operations and pay-as-you-go budgeting for reliable business continuity at a lower total cost.
- An infinitely scalable, vendor-neutral architecture that frees administrators from infrastructure management so they can focus on clinical workflow needs.

Hosted locally by the enterprise, the Clinical Collaboration Platform fosters efficiency and quality of care by providing seamless access to the collaborative imaging tools you need today, as well as the innovative tools of tomorrow. Hosted in the cloud by Carestream, it also frees your enterprise from the burden of hardware, application and security management – providing added peace of mind that your data is available only to authorized users, whenever and wherever they need it.

Appendix: Cloud Service Provider Checklist – How Secure Is Your Data?

1. *Physical Security*	Yes/No
Redundant utilities: power supply and air conditioning	
Fire and flood protection	
Ventilation: protection from temperature extremes and external pollution	
Windowless rooms for servers and storage	
Access control: biometric ID, visitor process, single entrance to sensitive areas, security cameras, auditing	
Scalable floor space	
2a. Application Level Availability	
Duplicate copy of data stored at multiple sites	
RAID-10 database storage	
RAID-6 data storage	
2b. Application Level Integrity	
Application-level signature and integrity check	
2c. Multi-Level Data Confidentiality	
Access control at site level	
Access control at user level, such as SRSA, secure ID and authentication	
Firewall	
Demilitarized zone (DMZ)	
Antivirus continuously updated with latest virus signature databases	
TSL/SSL-encrypted access tunnel	
3. Policy and Procedures	
Audit trail for activities related to patient health information (PHI)	
Proactive monitoring, 24/7	
Well-defined security policy	