CHECKLIST

5 things to consider when evaluating a cloud solution for clinical integration

HEALTHCARE

Cloud-based applications are commonplace in modern consumer and enterprise technology, but many healthcare organizations are concerned that the cloud is still not scalable, resilient, mature, or secure enough to handle their own clinical integration platforms. Luckily, there are many cloud options available today that are robust enough to meet the modern healthcare organization's needs, and many can be deployed with a flexible software-as-a-service (SaaS) model. As healthcare organizations begin to evaluate these options for clinical integration in the cloud, here are some of the most important questions to consider.

1. Is the cloud solution architected for resilience and availability?

A common reason why healthcare organizations move to the cloud is to maintain patient data continuity and avoid the issues that accompany system end-of-life dates. With a cloud integration solution, management and maintenance of the integration engine falls to the integration service provider, whose entire business model is structured around ensuring that hardware and software resources are operational and up to date.

Any SaaS solution you evaluate should meet the following requirements:

- Architected for resilience and availability
- Follows best practice designs
- Offers continuous patching and upgrades
- Includes automated testing
- Built from in-depth knowledge of cloud operations and healthcare integration
- Includes ongoing monitoring and reporting

2. What is the experience of the cloud provider, both in cloud operations and integration?

Cloud providers devote significant resources to ensuring their staff are well-versed in all relevant hardware and software technologies, new and old. Cloud providers also maintain comprehensive knowledge bases that include best practices and lessons learned by their technical staff, ensuring that institutional knowledge is maintained. Access to this technical expertise allows your organization to leverage the cloud provider's extensive knowledge and experience to keep your integration engine up and running.

When evaluating the expertise of a cloud provider, consider the following criteria:

- Educated in and follows best practice design
- Deep support bench with experience in integration, security, and healthcare needs
- Global experience in cloud operations
- Deep partnership with infrastructure/cloud service providers
- Ongoing investment and innovation in cloud and interoperability in the cloud

3. Can the cloud solution reliably grow with your organization?

Cloud solutions are specifically designed to scale alongside your organization's growth and varying workloads. They can also provide a unified view of all data and statistics across your connected health platform, giving your healthcare organization the company-wide data visibility it needs to make informed decisions about your integration platform.

When evaluating your cloud provider's ability to grow and scale with your organization, consider the following requirements:

- Presence of a scalable and reliable integration engine
- Experience in performance optimization, both for application and infrastructure
- Ability to increase transactional volume or additional functionality as the organization grows
- Capabilities to manage clinical and transactional data across your organization
- Infrastructure explicitly designed to support the needs of a clinical integration engine
- Scalability for high volumes of transactional data that does not incur unexpected costs or additional resources

4. Can the cloud solution mitigate security threats?

Today's quickly-evolving security landscape can make it very difficult for an organization's IT team to keep up with every potential new cyber threat. HIPAA-attested SaaS solutions offer the most secure environment to keep your health organization's PHI and PII safe. In a SaaS solution environment, the service provider manages infrastructure and application security, using dedicated resources to continually manage and update your systems for any security breaches and threats. This, in turn, enables a faster response to any potential problems or identified risks.

A potential SaaS provider should offer:

- Globally experienced security office with resources explicitly focused on data and systems security, particularly for organizations with rigorous healthcare security needs

- Training and tools to analyze existing services

- Regular updates for multiple levels of protection (including network- and host-based detection and protection)

- Application-level security, auditing, granular access control, and HIPAA compliance and attestation

5. How does the cloud solution provide a lower total cost of ownership?

On-premises solutions can incur extremely high costs, including infrastructure investments (at all levels), software maintenance costs, upgrade projects, and provisions for high availability capabilities. Over time, these can add up to much more than the cost of a cloud subscription for the same application footprint. Economies of scale make cloud software an economical choice for larger organizations, and can provide a significantly lower total cost of ownership (TCO) than on-premises solutions.

To ensure that a potential cloud solution will bring your organization substantial value, consider the following:

- Competitive pricing based on a transparent licensing model

- Size of vendor and strength of their cloud investments/partnerships

- Investment and innovation in the cloud integration solution that you would benefit from, such as FHIR and the broader API ecosystem

- Presence of teams dedicated to application implementation, cloud operations, security, and innovation beyond your organization's current capabilities

LEARN MORE ↗

Follow us: