cloudticity

10 Tips for Choosing a Cloud Management Partner for Healthcare



Choosing the right partner for cloud management is critical for your success as a healthcare organization. Whether you're just starting out in the cloud or you're looking to gain more value from your investment, the right cloud partner can increase your agility, enhance the quality of your services, and reduce the operating costs needed to sustain your business.

Choosing the wrong partner can do quite the opposite. Some cloud partners will slow you down, bottleneck your operations, make troubleshooting difficult, and even cause security and compliance gaps. When looking for a cloud management partner, look for these 10 things.

1. HITRUST certification status

Look for a healthcare cloud partner that maintains HITRUST CSF certification. While many cloud partners claim to be HIPAA compliant, studies have shown that 28% of vendors that claim alignment with HIPAA policies fail to meet those benchmarks. HITRUST certification is an extensive, third-party validation that ensures a vendor has met rigorous HIPAA and security requirements. A partner that does not uphold HITRUST certification could introduce risk to your organization.

2. Competencies and credentials

In addition to security competencies such as HITRUST, look for relevant cloud competencies. Amazon Web Services (AWS) provides a catalog of healthcare and government-related certifications that its partners can work to obtain, such as the Healthcare Competency and Public Sector Partner Competency, as well as validated technology competencies, such as the Audited Managed Service Provider credential and DevOps Competency certification. Microsoft also provides certifications for its cloud partners. When it comes to choosing an Azure partner, look for a partner that has achieved Gold or at least Silver status in multiple certification categories.

3. Business Associate Agreement (BAA)

A HIPAA BAA is a written contract between a HIPAA-covered entity and its vendors, contractors, and third-party service providers; it's required by law. BAAs describe how both parties adhere to HIPAA regulations and outline the responsibilities and risks each party takes on. Choose a partner that will sign a BAA and steer clear or any that won't. You can't be HIPAA compliant without a BAA.

4. Service Level Agreements (SLAs)

Ask about any SLAs the partner offers. What is their average ticket resolution time? Do they have 24/7 support SLAs for urgent production outages? If a potential partner can't guarantee that your help desk tickets will be resolved in a matter of minutes or hours instead of days, ask yourself what the cost of receiving slow service could be. Furthermore, if the partner doesn't have a 24/7 support SLA for production downtime, steer clear of this partner. You don't want to end up in an outage that you can't fix until business hours, putting your customers and brand at risk.

5. Relevant experience

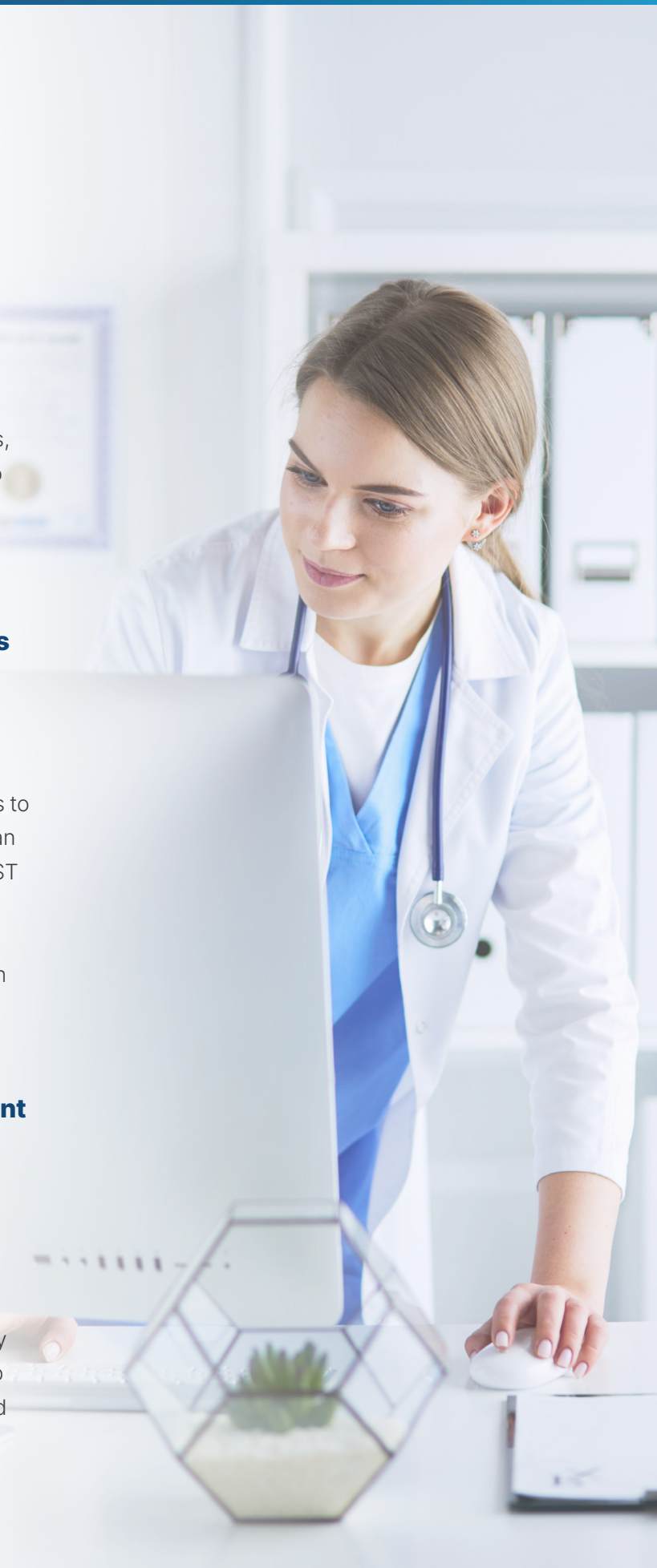
Many cloud partners can lay claim to being born-in-the-cloud or to having numerous years of cloud and healthcare experience. However, many of them are generalists. More important than years of experience are the years of relevant experience. Work with a partner that not only has extensive cloud experience, but specializes in healthcare and has deep expertise in the HITRUST CSF. They'll understand your business, know your unique challenges and risks, and be able to recommend HIPAA-eligible services while identifying industry trends.

6. Number of inheritable HITRUST controls

Some healthcare partners have developed code that allows you to fully or partially inherit HITRUST controls just by using their platform. Ask a prospective partner how many it has. If and when your organization decides to pursue HITRUST certification, the more controls you can inherit from your cloud partner, the easier your HITRUST certification process will be. Each inheritable control reduces the amount of work you have to do, reduces the timeline, and allows you to focus more resources on innovation and growth.

7. Control over your production environment

Ask a potential partner if they "black box" your environment, meaning do they require you to migrate to their own virtual private cloud (VPC) or can you own your own VPC? If you choose a partner that offers a black box model you will have to ask permission every time you want to make a change, reducing the flexibility and control you'll have over your environment. This also makes leaving the relationship a challenge and can lead to being locked into an expensive contract.



8. Automated services delivery

Operating in the cloud is unique to operating on prem because so many processes in the cloud can be automated via APIs. Automating cloud processes, such as patching or maintaining a strong password policy, reduces the risk of harmful human error or misconfiguration, which is the leading cause of breach in the cloud. Some cloud partners can automate 35% of their managed services delivery while others go as high as 99%. Ask a potential partner how much automation it employs. The more advanced the automation the tighter your security and compliance will be.

9. Services offered

Choose a partner that offers managed services, managed security, and managed compliance services at a minimum. But ask what other services they offer. Some cloud partners offer cloud cost optimization services as well. In addition, look for a partner that also provides a log management tool. Having a logging tool in place is required for HIPAA compliance, but third-party tools like Splunk and DataDog are expensive. You're better off getting logging included with your cloud management bundle.

10. Security track record

When it comes to managing and securing your PHI, you can't be too careful. In fact, cybersecurity attacks on healthcare organizations accounted for 79 percent of all attacks in 2020. And because of the high cost of recovering, about half of SMBs go out of business within six months after an attack. Make sure you do research on a potential partner and its track record. Choose a partner that has never experienced a breach or audit failure, and make sure the company has been around for more than several years.

While working with the right partner can improve your agility, security, and compliance, working with the wrong one can expose you to serious problems, slow you down, and increase your chance of a breach.

Reduce Your Risk and Increase Your Agility

Speak with a healthcare cloud expert today

SCHEDULE MY CONSULTATION

cloudticity

1301 Spring St Ste 25i • Seattle, WA 98104 • 855.980.2144 • cloudticity.com