HEALTHCARE CLOUD SECURITY

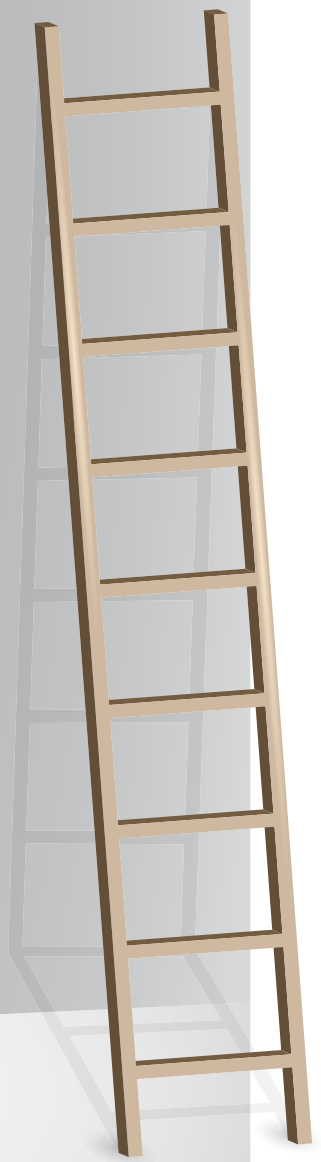
BUILD vs. BUY

... And Everything in Between

CLEARDATA™

BUILD VS. BUY

Security Strategies for the **Healthcare Cloud**



Contents

Healthcare technology has made remarkable significant strides in recent years and has improved the healthcare industry in many ways. Here are a few notable milestones.

This list contains just a few examples of innovations in healthcare technology and how they are transforming the broader healthcare landscape. These advancements pose both challenges and opportunities for healthcare organizations. Those orgs equipped with proficient in-house IT teams face a daunting array of factors when managing and ensuring the security and privacy of protected health information.

As data management increasingly migrates to the cloud, healthcare organizations are faced with a pivotal choices: Do I seek out a SaaS solution and manage it in house? Do I engage with an external SaaS solution and entrust my cloud security to a managed services vendor partner? Do I opt for an entirely do-it-yourself (DIY) approach and leverage my in-house team?

In this white paper, we will explore these options and key considerations to determine the optimal path forward for your organization.

Electronic health records (EHRs)

As the healthcare industry progresses, the transition from paper to digital platforms becomes more prevalent. Electronic health records empower medical professionals with the ability to access patient information from any location.[1]

Telemedicine

Telemedicine and remote medical services have drastically impacted the healthcare industry, specifically benefiting patients living in remote areas and, in many cases, improving health outcomes.[29] Nowadays, people can conveniently connect with their doctors through video calls, eliminating the need to travel for consultations. This innovative approach brings healthcare diagnoses and treatments right to their doorsteps, providing convenience and accessibility like never before.

Wearable medical devices [28]

Medical devices empower patients to capture and monitor their health in real-time, enabling seamless data sharing with their doctors. This proactive approach facilitates early detection of potential health issues, fostering timely intervention and care. Healthcare professionals and researchers are leveraging this data to transform patient care, diagnosis, and treatment. For instance, by analyzing patterns in the data, they can predict health trends, identify potential outbreaks, and personalize treatments.[2]

Improved diagnostics

Rapid advancements in technology have revolutionized diagnostics, elevating it in terms of accuracy, speed, and accessibility. The integration of cutting-edge diagnostic technology has emerged as a pivotal component in addressing one of the most critical aspects of healthcare, ensuring timely and precise identification of medical conditions for effective treatment and care.[3]

Artificial intelligence (AI)

AI has advanced by leaps and bounds, especially in the last year, and it is revolutionizing and improving the healthcare system. Among many of its capabilities, AI algorithms can analyze complex medical data and identify patterns that might be missed by humans. This can lead to more accurate diagnoses and better treatment plans.[4]

Improved Communication

Emerging technology in healthcare has facilitated improved communication within healthcare organizations. More and more medical professionals are leveraging technology to communicate effectively and efficiently about patients and their treatment to positively impact health outcomes.[5]

Stand-Alone SaaS, or SaaS + Managed Services for Healthcare Cybersecurity Operations?

Key considerations when debating whether to choose a SaaS only option versus using a vendor's managed services together with your chosen software solution

Choosing a Stand-Alone SaaS Solution

A stand-alone SaaS solution provides software functionality delivered over the cloud that gives an organization more hands-on control over its operations with little to no delay in time to implementation.[17] Typically, you can begin to use the software immediately without waiting weeks or months to deploy it. Cloud-based SaaS services can also scale relatively easily as a business grows and as needs change.[20]

With a standalone, cloud-based SaaS, organizations avoid the cost of installing software on legacy systems. A DIY SaaS can offer a more simple and cost-effective pricing model than most managed services options.[19] It's ideal for teams that already have a strong in-house bench of IT and cloud cybersecurity and related healthcare expertise who can manage both the day-to-day and longer-term needs of their security and compliance in the public cloud, including discovery, automation, enforcement, and remediation.[18]

Choosing SaaS + Managed Services

Managed services offer a more comprehensive approach to IT management of your cloud environment. As opposed to a DIY SaaS, organizations using managed services have more control over implementation, ongoing support, and assistance addressing unique security challenges.[20] Going the managed services route provides a holistic solution that encompasses software management, hardware support, and IT strategy transformation.[21]

Managed services extend beyond traditional software management to include hardware support.[22] By outsourcing tasks like maintaining security on IT networks, healthcare organizations can benefit from expert recommendations to upgrade and improve their hardware infrastructure. For example, managed security services may recommend replacing ailing servers with cloud-based services, ensuring optimal performance and scalability.[23]

One of the key advantages of managed services is the ability to identify opportunities for integration and process improvement. For instance, by linking cloud-delivered plugins for a healthcare organization's website, managed services enable immediate communication between sales representatives and customers through a website chat app, improving customer engagement and satisfaction.[24] [25] [26]

Deciding Between DIY & Outsourcing

Another side of the coin is the decision to manage all healthcare cloud cybersecurity operations in house or engage an external vendor partner for services. Below are key considerations for healthcare organizations.

Budget constraints

Consider both short-term and long-term financial implications. Beyond software expenses, there's an ongoing need for full-time staff dedicated to cloud security and management. SaaS is typically not regarded as a capital expenditure, which implies that the principal cost of such a project will predominantly be considered an operational expense.[6] This is an important factor to bear in mind when considering the budget constraints associated with a DIY SaaS solution.[15] If financial limitations are a concern, organizations should cautiously weigh the option of a DIY SaaS solution — provided, of course, that you have the right team in place to manage it effectively.

Resources & expertise

Your existing staff's capabilities are a linchpin in determining the best path forward. Evaluate their expertise — not only in general IT but also in the specialized areas of cloud security and compliance. Determine whether they possess the necessary skills to efficiently implement and manage a cloud security posture management (CSPM) solution. Furthermore, consider whether your team has the bandwidth to accommodate the demands of continuous cloud infrastructure management, including round-the-clock monitoring and remediation. Beyond merely the expenses related to the software, there exists a continuous necessity for dedicated full-time staff for cloud security and management. The cost of maintaining such a team can significantly add up over time, influencing the total cost of ownership of the SaaS solution.

Cloud maturity & legacy systems

Cloud maturity refers to an organization's readiness to migrate its data and operations to the cloud. It encompasses the technical capabilities, security measures, staff proficiency, and overall cultural readiness of the organization to make such a transition.[7] Cloud maturity plays a significant role in the decision-making process for data management solutions.[8] Gauge your organization's level of familiarity with cloud technology, as it significantly influences your approach. If your organization has an established presence in the cloud, a DIY solution may align with your experience.

Additionally, you must consider whether your legacy systems are up to par when it comes to security and compliance? Many legacy data systems vendors eventually stop offering security updates, leaving systems vulnerable to evolving threats. Is this the case for your legacy systems? It's possible that your systems lack essential security features like multifactor authentication, potentially leaving sensitive patient data exposed. Inadequate security measures not only put patient data at risk, but also expose your organization to potential legal and regulatory compliance issues. Such shortcomings are particularly concerning when they pertain to your legacy electronic health record (EHR) software. Any exposure of protected health information (PHI) puts you in jeopardy of experiencing a data breach, along with its potentially substantial financial and reputational repercussions.

Scalability

Think about your organization's growth trajectory. For smaller startup companies aiming to expedite their entry into the cloud, a DIY solution may be a viable option. Depending solely on your in-house team, even if they are skilled, can pose challenges. They may struggle with 24/7 cloud monitoring, potentially leading to delayed responses to vulnerabilities.[9] As the company grows, you'll need to grapple with tough decisions about where to allocate resources.[10] Do you prioritize your tech stack, ensuring it can support your growth effectively? Or do you lean more into business expansion? Regulations often mandate a focus on the tech stack, which adds another layer of complexity to the equation.[11] Do you find yourself needing to choose between business objectives and managing security and compliance in house?

While on-premise solutions may feel as though they provide a higher degree of control when securing data residing within the company's physical location, it requires significant upfront investment, ongoing maintenance, and can limit scalability. The ability to physically lock your data room doesn't always mean it's more secure.

Deciding Between DIY & Outsourcing

Risk tolerance

In the healthcare industry, safeguarding sensitive data and patient trust is paramount. Before making any decisions, it's important for healthcare organizations to carefully evaluate their risk tolerance — particularly considering the impact that data breaches can have on brand reputation and patient trust and safety.[12] Managed services can function as an extension of your team, shouldering responsibilities such as deployment, maintenance, monitoring and response to security threats.[13] However, if your in-house team possesses the necessary capabilities to independently manage potential security risks, a DIY solution can streamline security processes.

After considering these six factors, you should assess whether your organization is positioned to manage your cloud strategy in-house or if you should consider support from managed services, Even if you are equipped to DIY, using a platform built for healthcare organizations will optimize your internal team, enabling them to do more with less.

Compliance vs. Security

While compliance and security are different, they are closely related and vital against relentless cybersecurity attacks in healthcare. To be compliant with regulations like HIPAA, healthcare organizations need to have robust security measures in place. But just because an organization is secure doesn't necessarily mean it's compliant.[16] A DIY solution can facilitate continuous compliance using automation and remediation, though human expertise is still an invaluable asset. The complexity of healthcare regulatory requirements demands a careful evaluation of whether your in-house team possesses the expertise necessary to navigate these intricacies. Remember, compliance doesn't necessarily mean secure.[15]

Questions to Ask a Cloud Security Vendor

Whether you've reached a decision between a SaaS solution or a SaaS with managed services, or you're still considering which route to take, here are the questions you can ask cloud vendors to support your decision and help you choose the right partner for your needs.

- How can you as a tech vendor effectively address providers' and hospitals' concerns about cloud security?
- How much day-to-day control do I really need in the protection of my data and will a standalone software solution provide the necessary customization and flexibility?
- Do I need a CNAPP or CSPM solution for my business?[14]
- How long will implementation take? How quickly can I implement and integrate a CSPM solution? Will my team be able to handle the implementation process efficiently?
- How much support do I need? Can my team effectively handle the daily management and maintenance of the CSPM solution, or should we depend on the expertise and support of managed services?
- Does this DIY solution meet my needs? How does it address my organization's unique security challenges? Is it healthcare specific or for multiple industries? Can it adapt to our specific compliance and security requirements
- What are the risks and benefits? What should we consider as concerns versus value-adds for each approach? How can a cloud partner mitigate the risks and maximize the benefits?
- What healthcare-specific expertise can you offer my team, and can you keep pace with the stringent healthcare regulatory environment?
- Does your organization have a multi-cloud solution?
- How can you support me with audit-ready reporting capabilities?
- How can your organization help me identify where exactly PHI lives in my database?
- Can your organization provide me with the flexibility and partnership I need as my business grows and my objectives evolve?

ClearDATA: Your All-in-One Healthcare Cloud Cybersecurity Solution

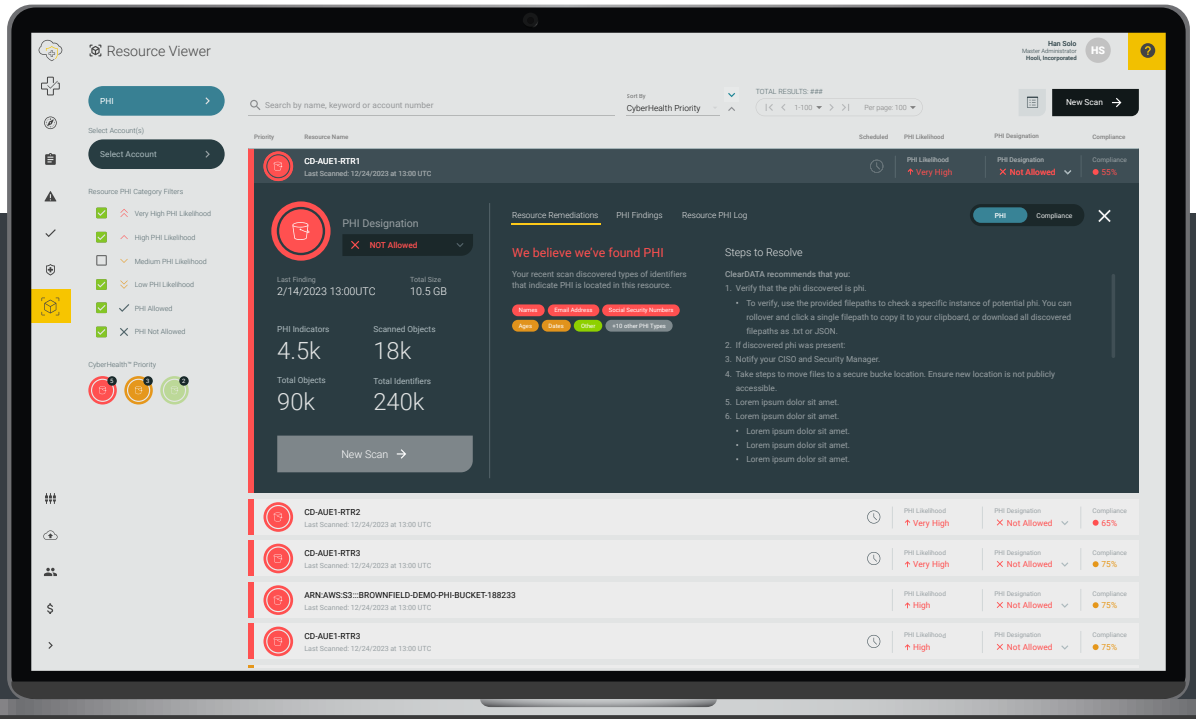
We maintain continuous security and compliance for full visibility, protection, and enforcement of security and compliance measures in the public cloud. Our cloud security posture management (CSPM) and Managed Detection & Response (MDR) software and services are purpose-built to protect PHI and other sensitive healthcare data.

Whether you choose our SaaS CSPM software, the CyberHealth™ Platform, as a software-only solution or opt for managed cloud services, ClearDATA empowers you to make an informed decision based on your budget, resources, and specific requirements. By partnering with ClearDATA, you can confidently safeguard your cloud infrastructure and focus on protecting sensitive patient information, growing your business, and innovating in the cloud.

The decision to build internally versus partner with an expert is complex. At ClearDATA, we meet you where you are in your cloud journey.

KEY TAKEAWAYS

1. *Healthcare is rapidly evolving and innovating.*
2. *Consider where your business is currently on its cloud journey.*
3. *Ask the right questions of any vendor you help you consider whether DIY or outsourcing will help your business grow.*



References

1. Concord University. (n.d.). How Technology Has Advanced Health Care. Retrieved from [https://www.concorde.edu/blog/how-technology-has-advanced-health-care]
2. The Medical Futurist. (n.d.). Ten Ways Technology Is Changing Healthcare. Retrieved from [https://medicalfuturist.com/ten-ways-technology-changing-healthcare]
3. Retinal Screenings. (n.d.). Top Benefits of Technology in Healthcare. Retrieved from [https://retinalscreenings.com/blog/top-benefits-of-technology-in-healthcare]
4. Fingent. (n.d.). 7 Major Impacts of Technology in Healthcare. Retrieved from [https://www.fingent.com/blog/7-major-impacts-of-technology-in-healthcare]
5. The Manufacturer. (n.d.). 6 Ways Technology Is Transforming the Healthcare Industry. Retrieved from [https://www.themanufacturer.com/press-releases/6-ways-technology-transforming-healthcare-industry]
6. CMSWire. (n.d.). Understanding the Financial Implications of a SaaS DAM. Retrieved from [https://www.cmswire.com/cms/digital-asset-management/understanding-the-financial-implications-of-a-saas-dam-025051.php]
7. Veritis. (n.d.). Cloud Computing Maturity Model. Retrieved from [https://www.veritis.com/blog/cloud-computing-maturity-model]
8. Google. (n.d.). Cloud Maturity. Retrieved from [https://digitalmaturitybenchmark.withgoogle.com/cloud]
9. CloudZero. (n.d.). The Benefits of Cloud Scalability. Retrieved from [https://www.cloudzero.com/blog/cloud-scalability]
10. Hewlett Packard Enterprise. (n.d.). What Is Cloud Scalability? Retrieved from [https://www.hpe.com/us/en/what-is/cloud-scalability.html]
11. ClearDATA. (n.d.). 6 Considerations for Evaluating DIY Cloud Management. Retrieved from [https://www.cleardata.com/6-considerations-for-evaluating-diy-cloud-management]
12. National Center for Biotechnology Information. (n.d.). Cloud Computing in Healthcare: A Comprehensive Survey. Retrieved from [https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6561516]
13. SecurityScorecard. (n.d.). Effective Healthcare Risk Management System. Retrieved from [https://securityscorecard.com/blog/effective-healthcare-risk-management-system]
14. ClearDATA. (n.d.). CSPM Pillar Page. Retrieved from [ClearDATA CSPM Pillar Page]
15. Healthcare IT News. (n.d.). Security vs. Compliance: What's the Difference? Retrieved from [https://www.healthcareitnews.com/sponsored-content/security-vs-compliance]
16. AuditBoard. (n.d.). Security vs. Compliance: Understanding the Differences. Retrieved from [https://www.auditboard.com/blog/security-vs-compliance]
17. CircleCI. (n.d.). Top 6 Advantages of SaaS. Retrieved from [https://circleci.com/blog/top-6-adv-of-saas]
18. Saasholic. (n.d.). Understanding SaaS Benefits and Challenges. Retrieved from [https://saasholic.com/understanding-saas-benefits-and-challenges]
19. Acropolium. (n.d.). Benefits of SaaS Software Solutions for Small and Medium-Sized Businesses. Retrieved from [https://acropolium.com/blog/benefits-of-saas-software-solutions-for-small-and-medium-sized-businesses]
20. Insight. (n.d.). Managed Cloud Services. Retrieved from [https://www.insight.com/en_US/content-and-resources/glossary/m/managed-cloud-services.html]
21. CIO. (n.d.). 6 Top Managed Cloud Services Providers and How to Choose. Retrieved from [https://www.cio.com/article/405257/6-top-managed-cloud-services-providers-and-how-to-choose.html]
22. Deloitte. (n.d.). Cloud Managed Services. Retrieved from [https://www2.deloitte.com/us/en/pages/technology/solutions/cloud-managed-services.html]
23. Red Hat. (n.d.). What Are Managed IT Services? Retrieved from [https://www.redhat.com/en/topics/cloud-computing/what-are-managed-it-services]
24. Cloudian. (n.d.). Managed Cloud Services: What Are They and How Do They Work? Retrieved from [https://cloudian.com/guides/hybrid-cloud/managed-cloud-services]
25. Cognizant. (n.d.). Cloud Managed Services. Retrieved from [https://www.cognizant.com/us/en/glossary/cloud-managed-services]
26. HTL. (n.d.). The Role of IT Managed Services in Cloud Computing. Retrieved from [https://www.htl.london/blog/cloud-computing-role-of-it-managed-services]
27. McKinsey & Company. (n.d.). The Big Data Revolution in US Health Care. Retrieved from [The Big Data Revolution in Healthcare - McKinsey Media Kit PDF]
28. Newsweek. (n.d.). US Healthcare Systems Should Adopt Rapid Innovation Hubs. Retrieved from [https://www.newsweek.com/us-healthcare-systems-should-adopt-rapid-innovation-hubs-1800007]
29. Centers for Disease Control and Prevention. (n.d.). Telehealth in Rural Communities. Retrieved from [https://www.cdc.gov/chronicdisease/resources/publications/factsheets/telehealth-in-rural-communities.htm]

CLEARDATA™

MKT-0123 Rev. A, Jan 2024