7 Steps to Hospital Cloud Security Success

Practical tips for achieving flexible, scalable protection for your hospital’s staff and sensitive data
# Table of Contents

<table>
<thead>
<tr>
<th>Step</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>03</td>
<td>Introduction</td>
</tr>
<tr>
<td>05</td>
<td>Develop a Comprehensive Cloud Strategy</td>
</tr>
<tr>
<td>06</td>
<td>Define New Security Policies, Procedures and Controls</td>
</tr>
<tr>
<td>07</td>
<td>Draw Clear Lines of Responsibility</td>
</tr>
<tr>
<td>08</td>
<td>Review the Cloud’s Configuration</td>
</tr>
<tr>
<td>09</td>
<td>Create a Cloud-specific Security Reference Architecture</td>
</tr>
<tr>
<td>10</td>
<td>Accept Responsibility For Compliance</td>
</tr>
<tr>
<td>11</td>
<td>Continuously Scan and Monitor Your Cloud Environment</td>
</tr>
</tbody>
</table>
Introduction

When it comes to the cloud, IT and security professionals have mixed feelings. While 75% of them view the public cloud as more secure than their organization’s own data centers, 92% don’t believe they are well-prepared to secure these cloud services.¹

For hospital security teams, the prospect of protecting data in the cloud is, at the very least, unsettling. Securing data in someone else’s data center—without having any physical access to the underlying infrastructure—isn’t something they’d eagerly raise their hands to do.

However, COVID-19 has changed things. To support telemedicine and other remote applications, hospitals have quickly turned to the cloud.

¹ KPMG and Oracle Cloud Threat Report 2020
Introduction

Pandemic conditions have urged more hospitals to embrace the cloud. HIMSS reports cloud adoption has doubled since 2018, with 58% of healthcare IT workloads and infrastructure now in the cloud.² This is a hefty increase.

According to IDG, this steep adoption curve is less about cost savings and more about the cloud’s other advantages, such as faster application provisioning and enhanced computing power.

Of course, not all hospitals are enthusiastically embracing the cloud. There are still skeptics who ask, “Is the cloud secure?” But for security teams, the more relevant question is, “Are we using the cloud securely?”

Signs your cloud footprint is not secure:

→ **Continued data loss**: Healthcare has experienced a 58% increase in industry data breaches this year.³

→ **Misconfigured cloud services**: Led by overprivileged accounts, exposed web servers and other types of server workloads, misconfigurations remain the most prevalent cloud vulnerability.⁴

→ **Many specialized cloud security tools**: 70% of organizations say too many specialized tools are needed to secure the public cloud footprint (more than 100 discrete products on average).⁵

→ **Compromised cloud credentials**: 59% of organizations have experienced spear phishing attacks that compromised employees with privileged cloud accounts.⁶

→ **Fast deployments**: Hospitals that bring new sites online without waiting for carrier provisioning create security risks.

→ **Rising cloud costs**: Through 2024, 80% of companies that are unaware of their cloud adoption mistakes will overspend by 20-50%.⁷

². Advisory Board, “COVID-19 is pushing healthcare into the cloud,” 2020
³. Verizon’s 2020 Data Breach Investigations Report
⁴. Migrating Cloud Vulnerabilities, the U.S. National Security Agency (NSA), 2020
⁵. Oracle and KPMG Cloud Threat Report 2020
⁶. Oracle and KPMG Cloud Threat Report 2020
⁷. Smarter with Gartner, “4 Lessons Learned From Cloud Infrastructure Adopters,” June 30, 2020
Seven Steps to Hospital Cloud Security Success

Step 1: Develop a Comprehensive Cloud Strategy

Do you have isolated cloud initiatives scattered across your hospital or health system? Form a group with a broad range of participants to help create cloud guidelines for your entire organization. Be sure each of these guidelines connects directly to your hospital’s business strategy. Remember to include distinct objectives, benefits, risks, and key criteria for adoption and compliance in your guidelines.

A cloud strategy is not an implementation or migration plan. Rather, it should pave the way to cloud adoption by providing a clear perspective on the cloud and its role in your hospital.

Think of your cloud strategy as a living document. It will change as vendors come and go, the healthcare landscape changes, and organizational goals shift and develop.
Step 2: Define New Security Policies, Procedures and Controls

Don’t assume you can lift and shift your on-premises privacy and security controls because they may not be designed to protect your data against cyberattacks in a public cloud environment.

In fact, misconfiguring your cloud security controls can very well open the door to cyberattacks. Gartner predicts through 2025, 99% of cloud security failures will be the customer’s fault. The first step to avoiding this outcome is to get visibility into your current state of security on-premises and across private and public clouds. Then, get a clear picture of your CSP’s security practices.

Cloud security tip: Before the contract phase, ask them to fill out a Consensus Assessment Initiative Questionnaire (CAIQ) developed by the Cloud Security Alliance. This assessment will give you valuable insight into the CSP’s security practices.

If you have a Cloud Center of Excellence to manage and govern cloud adoption, collaborate with this group to ensure your policies and procedures are optimizing the security and reliability of the architectures that are slated for deployment.

Step 3: 
Draw Clear Lines of Responsibility

Because cloud security is a shared responsibility between you and your CSP, it can be difficult to nail down who is doing what. This becomes even more complex when hosting healthcare information in the cloud. The HIPAA Security Rule alone has more than 50 standards and implementations to be split between your hospital and your CSP.¹

On a very basic level, CSPs are responsible for securing the cloud environment, and you’re responsible for protecting what’s in the cloud—including your patient and medical data. You’re also accountable for securing your staff and their behaviors, including compliance failures caused by their actions or inactions.

The division of specific security responsibilities between your hospital and your CSP will be slightly different, depending on your chosen route to the cloud. (See the chart at the right.)

→ **Infrastructure as a Service (IaaS)** involves changes to the architecture, such as lifting and shifting an existing application to be hosted in the cloud.

→ **Platform as a Service (PaaS)** involves changes in functionality, such as rebuilding an application so it can leverage the cloud to lower costs and accelerate iterative improvements.

→ **Software as a Service (SaaS)** involves changes to the ways applications are delivered, accessed and managed, such as using the web to deliver and access third-party applications.

¹ "Cloud security demands a shared strategy for HIPAA Compliance," Healthcare IT News, 2020

### Cloud Security Responsibility

<table>
<thead>
<tr>
<th>Asset to be protected</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Data</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Apps</td>
<td>●</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>Operating System</td>
<td>●</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Virtual Networks</td>
<td>●</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Hypervisors</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Servers and Storage</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Physical Networks</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

You ● Cloud Service Provider ○

Regardless of the route you choose, it’s imperative to work closely with your CSP to confirm who is responsible for which security elements. After an initial agreement is reached, continue to collaborate with your CSP to clarify your obligations as your hospital’s cloud usage changes/evolves.
Step 4: Review the Cloud’s Configuration

Misconfigurations are one of the errors most commonly associated with cloud security incidents. In fact, organizations with known misconfigured cloud services experienced 10 or more data loss incidents last year.\(^\text{10}\)

Although your CSP will provide configuration guidance and controls, it’s important to make sure the cloud’s hardware and software details are set up for interoperability and communication across your staff’s various locations. Also check your CSP’s configurations to confirm they’re compliant with NIST, HITRUST, CIST, HIPAA, GDPR, and other applicable healthcare standards and government regulations.

\[\text{Need help? Cloud configuration monitoring tools are available that can help you identify misconfigurations. You can also use network traffic monitoring and user behavior analytics to identify anomalies and misconfigurations, along with their associated issues.}\]

\(^\text{10\,Oracle and KPMG Cloud Threat Report 2020}\)
Step 5: Create a Cloud-specific Security Reference Architecture

To safely place workloads in the cloud, you’ll need to build a cloud-specific security reference architecture incorporating these components:

→ **Identity access management.** Identify and define the users who are authorized to operate in the cloud environment, including users, privileged users, patients, devices, applications, and provisioning access. Spell out what they’re allowed to do. Consider adopting a Zero Trust Network to secure your remote staff, replacing implicit trust with explicit verification, every time.

→ **Application security.** Establish a collective understanding of applications in use and their corresponding threats. To simplify this process, you can implement a Cloud Access Security Broker (CASB) to secure SaaS, PaaS, IaaS and homegrown applications. As a preventative measure, you might also consider moving to a DevSecOps model, embedding security into the entire application lifecycle.

→ **Data security.** To ensure the secure storage and sharing of sensitive patient data, invest in FIPS 140-2 and HIPAA-compliant tools that give you complete control over where data resides, as well as when and with whom it is shared. Determine the scope of AES-256 encryption for data-at-rest and data-in-motion. Activate each of the cloud provider’s key management services and private key management, in addition to strong authentication and policy-based data loss prevention (DLP) controls for storage and collaboration.

→ **Data activity monitoring.** Log and audit all data activity at a granular level to comply with your hospital’s security policies and applicable regulations.

Of security professionals say the pandemic has accelerated their Zero Trust efforts.  
(Deloitte poll, 2020)

Addressing these areas will help create a robust foundation for keeping your data secure in the cloud.
Step 6: Accept Responsibility For Compliance

Most CSPs use third-party audits to continually evaluate their regulatory compliance. However, your CSP’s compliance doesn’t cover your use of the cloud environment. As a result, you should not only assess your CSP’s security practices, but also develop and maintain additional controls that coincide with your security risk management framework.

With the right technologies, this can be simpler than it sounds. Using large libraries of prebuilt templates, some DLP tools can automate your compliance specific to your region, government and industry regulations.

Compliance tip: Familiarize yourself with the HiPAA Privacy, Security and Breach Rules and how they apply to the cloud. For details, refer to “Guidance on HiPAA and Cloud Computing” by the U.S. Department of Health and Human Services.

Trust program certifications—not just self-audited compliance. Be wary of CSPs that claim certification for their entire organization, yet only include a single subset of operations in the compliance scope. Become familiar with ISO 27001, ISO 27018, CSA STAR, SOC 2 Type 2 certifications, which will help you identify potential security control issues.
Step 7: Continuously Scan and Monitor Your Cloud Environment

Even when you’ve completed your cloud deployment, your work is still not done. Actually, you’re just getting started. Unlike monitoring a static data center, the cloud is a rapidly changing environment. To monitor it effectively, you’ll need:

→ **The ability to observe behaviors** at every level of your cloud infrastructure, including visibility into the host, container, control plane and application layer.

→ **Deep behavioral context for alerts** so you clearly understand what has happened and whether it’s truly an anomaly for a specific user or entity. This will help combat alert fatigue. You can also quickly prioritize high-risk incidents with risk scoring, which is included in some behavior analytics security solutions.

→ **A security posture assessment** of users and non-human entities to determine incorrectly provisioned or over-provisioned high-risk privileges. This adds a preventative dimension to your hospital’s cloud security.
Flexible protection for your hospital in the cloud

By following the seven steps outlined in this ebook, you’ll be several steps ahead of your peers in protecting your hospital in the cloud. As you develop your strategy and define new policies, be sure to explore new technologies that will help you put these plans in action. (You won’t be able to rely on static security tools to protect the cloud’s dynamic environment.)

At Forcepoint, we believe the best way to secure the cloud is with the cloud. To achieve flexible, scalable protection for your hospital, we recommend Forcepoint Cloud Security Gateway (CSG). CSG delivers web, cloud and data security in a cloud-based, centrally managed service. It flexes to protect your critical data and your teams as they care for patients in new ways. In addition, CSG:

→ Secures your remote staff’s access to on-premises patient/medical data and business-critical cloud applications.

→ Stops malware, viruses and phishing, wherever your staff is working.

→ Uncovers risky cloud applications and Shadow IT while securing cloud access across your organization.

→ Delivers complete web and data protection with uniform policies for every user everywhere.

→ Provides controls for BYOD, managed devices and real-time compliance.
If you have any questions about CSG or any of the steps in this ebook, we’re here to help!

Contact Us

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint’s humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.