CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Keeping Patient Data Secure in the Cloud

In the past three decades, cloud computing as we now know it has undergone many changes. Long gone are the days where large corporations had a single off-site server parsing data. Today, businesses of all sizes are embracing the cloud for storage to services and beyond.

While we've seen increased cloud adoption in the last three or four years, cloud usage—and a rapid acceleration into cloud services—has increased across many industries, including healthcare.

In fact, Microsoft CEO Satya Nadella is quoted in a January 2021 **Forbes article** that within just a few months of the pandemic, the company had seen the equivalent of two years of digital transformation as a growing number of its customers adopted cloud solutions.

Likewise, in late 2021, Gartner estimated that global cloud revenue is likely to reach **$474 billion** in 2022, up from $408 billion the previous year. That same report goes on to estimate that more than 85% of organizations will embrace a cloud-first principle by 2025.

For healthcare specifically, the **Healthcare Cloud Computing – Global Market Trajectory & Analytics** report estimates the industry's global cloud computing market is expected to reach almost $77 billion by 2026.

IT'S NOT ALL OR NOTHING

When it comes to cloud migration, there has long been a misconception that your organization must take an all-or-nothing approach. There's long been a traditional view that to even begin this journey, your organization must develop a detailed plan that encompasses the entire migration process (think all of your systems, data, applications and services across your entire organization, regardless of criticality or dependencies).

This has often looked like a stepped approach, often in this order:

- Waterfall process (complete all design before starting migrations)
- Sequential delivery (hand-offs) of infrastructure build, middleware configuration, code deployment, network configuration and testing
- Architecture teams operate separately from engineering, test, networking and security

In this traditional approach, teams often get so overwhelmed by the details, costs and timeframes, that they just give up and choose to do nothing instead of tackling it all. But, as we've seen the pandemic force healthcare organizations to think about services and delivery models in a new way, cloud adoption no longer has to be an all-or-nothing strategy.

Instead, more controlled, incremental migration to the cloud can help your organization achieve efficiencies while meeting goals and delighting customers. Instead of focusing on the "all," a more modern approach takes into consideration the capabilities and productivity of your teams and then empowers them to make digital transformation decisions that flywheel your organization to success.

There are a number of benefits to this more controlled approach. It enables your teams to:

- Tackle the volume of change your teams can handle
- Prioritize migration projects that unlock the most value for your organization
- Make decisions
- Embrace a mindset of data-driven, continuous improvement
- Focus on incremental change
- Use performance data and feedback to inform modernization and optimization decisions

Think of it like this: Your teams are smaller cogs that help turn the larger cloud transformation wheel. As each smaller cog functions at optimized levels, you can model that success and expand it into larger environments. From there,

you can continuously scale up, starting first with your most critical and important services and data and moving upward from there.

So, how would you scale your cloud transformation program once you've set this pace? Consider:

- Launching detailed on-premises discovery to collect baseline dependency, sizing and performance dates for the entire environment
- Establishing program, governance and factory operating modes
- Assigning core teams and launching sprint planning for the first one or two portfolio groups to move next, and begin planning for portfolio segment migration sequencing over the course of the full program
- Beginning detailed design on complex applications ("big rocks") for initial portfolio move groups
- Set up an SME team to assess entire portfolio for systems with tight coupling to mainframe and midrange systems
- Begin development of a plan to decouple, resolve or remove these dependencies

WEIGHING CLOUD BENEFITS AGAINST RISKS

While the pandemic may have accelerated cloud usage and changed our views on the all-or-nothing migration approach, many healthcare organizations have been working on a full or hybrid cloud model for years. That's because using the cloud brings a lot of advantages to organizations, from cost-savings to scalability, often with less resources required to manage on-site architecture.

As more and more organizations migrate data to the cloud, there is a growing sense of (false) security that data in the cloud is always safe. While that may be true in some instances, when we're talking about patient data and all of the requirements and regulations that surround security and privacy, the reality is there are increasing chances your sensitive data could be exposed to the public. This is especially true in a public cloud model, for example, Amazon Web Service (AWS) or Microsoft Azure. As you increase your cloud usage, so increase your risks.

To add an additional layer of complexity, some healthcare organizations don't have a good understanding of who is responsible—the healthcare organization or the cloud provider—for ensuring that data is protected and secure.

In many instances, it's a shared responsibility model. That means depending on the agreement, both the organization and the cloud services provider have responsibilities.

In an example with a public cloud model, your healthcare organization may be responsible for security in the cloud, such as:

- Customer data: How it's stored, shared and accessed
- Platform, applications, identity and access management
- Operating systems, networks and firewall configuration
- Client-side data including encryption and data integrity, as well as authentication
- Service-side encryption, such as file systems and data
- Network traffic protection such as encryption and data integrity

While each organization's needs are specific, in general, your healthcare organization should retain ownership and control of:

- Data hosted on the cloud
- Who accesses content and services
- Which level of security is appropriate for the data
- Which services are employed
- Configuring the environment in a way that conforms with applicable regulatory requirements

Similarly, in this shared-responsibility model, the cloud-services provider may be responsible for security of the cloud, such as:

- Software: Computer, storage, databases, networking
- Hardware/infrastructure: Regions, availability zones, edge locations

THE IMPACT OF DATA BREACHES

As healthcare organizations continue migration to the cloud, many do so with some trepidation. According to **Sophos State of Cloud Security 2020 report**, some 96% of respondents had concerns about public cloud security and about 70% that host data or workloads in a public cloud have experienced a breach, most commonly malware.

Common Cloud Breach Types

Malware **(34%)**

Exposed data **(29%)**

Ransomware **(28%)**

Account compromises **(25%)**

Crypto-jacking **(17%)**

Source: https://secure2.sophos.com/en-us/content/state-of-cloud-security.aspx

These breaches may often be the result of not understanding risk factors that exist in cloud environments. While this list is not exhaustive, some common risk factors are related to:

- Insufficient identity and credential management
- Easy registration systems, phishing and pretexting
- Insecure APIs
- Misconfigurations
- Insider threats
- Account hijacking via stolen credentials
- Denial of service (DoS) attacks
- Malware

While there are no fool-proof ways to ensure your organization won't experience a breach, there are some best practices you can implement to help decrease your risks. Here are a few tips:

- Develop company-wide cloud usage and permission policies
- Require multi-factor authentication (MFA)
- Implement data access governance
- Enable centralized logging to make it easy for investigators to access the logs during an incident
- Implement data discovery and classification
- Enable user behavior analytics
- Establish data remediation workflows
- Implement data loss prevention (DLP)

MISCONFIGURATIONS AND THE VALUE OF STRONG CLOUD CONFIGURATION

Misconfiguration issues continue to increase risk for cloud environments. According to the **State of Cloud Security 2021 report published by Fugue**, misconfigurations are the No. 1 cause of cloud breaches and nearly a third of respondents say they're concerned that misconfiguration rates will increase in the next year. The report also goes on to highlight that the number one cause of cloud misconfiguration is generally APIs and interfaces that require governance.

Unfortunately, these issues can often be overlooked or go undiscovered until a breach happens. About 83% of the survey respondents said they're concerned their organization is at risk and some 36% have experienced a serious cloud data leak or breach within the past 12 months.

But you don't have to be caught off-guard. Understanding common misconfiguration issues

and why strong cloud configuration practices are important can help you thwart a future attack.

When it comes to risks in the cloud, there are some common risk factors for misconfigurations to be aware of. These may include:

- Human error
- Excessive permissions
- Maintaining unused and stale accounts
- Allowing excessive sharing settings, which can lead to sensitive data being overexposed
- Leaving default settings unchanged, including admin credentials and ports
- Disabling standard security controls
- Not enabling encryption

While risk awareness is important for cloud security, you can also implement some best practices to help mitigate your misconfiguration risks such as:

- Establishing baseline configurations and regularly conducting configuration auditing
- Using continuous change monitoring to detect suspicious changes and investigating them promptly
- Requiring data owners to periodically attest that permissions match employees' roles
- Assigning user groups
- Limiting and validating that all access rights align data protection

Additional recommendations to help promote a strong cloud configuration model include:

- Identity and access management (IAM) capabilities: Ensuring the right people have the right level of access to your cloud environment, for example, adopting the principle of least privilege so they can't access more than they need to for their specific role/responsibility. This might also include adopting groups and rules to regulate what certain users can and cannot do within your cloud environment.
- Multi-factor authentication (MFA)
- Secure network configuration

- Data security
- Logging and monitoring
- Customizable alerts

While all of these activities can help shore up your cloud configuration, it's worth noting that many of these activities should be customized for your organization's specific needs. For example, the cloud won't automatically encrypt your data. That's a responsibility that may fall to your organization. While logging and monitoring tools may be available, they won't often be automatically enabled, so you will need to set those up. Same for those valuable alerts that let you know when security issues come up.

REDUCING INSIDER THREATS

Insider threats continue to increase risks for cloud security, and there are a range of insider threat risk factors for healthcare organizations today. And while insider threats can be intentional, such as a disgruntled employee, or unintentional, such as human error, your employees aren't the only "insiders." You also face risks from your contractors, suppliers and partners who can also access data inappropriately, expose it, or cause it to be stolen. Unfortunately, many enterprises lack visibility into user and admin activity across their cloud platforms, making them increasingly susceptible to these risks.

However, there are some steps your organization can take to help mitigate risks caused by insider threats. Consider:

- De-provision access to resources immediately whenever you have personnel changes
- Seek out signs of suspicious activity trends
- Monitor privileged users
- Track service and privileged accounts separately from other user accounts
- Implement user behavior analytics
- Create a baseline behavioral profile of each user and watch for actions atypical for that user or others with the same role
- Track attempts to access disabled accounts, along with any other anomalous attempts to access data or gain elevated permissions

CLOUD SECURITY BEST PRACTICES

With the pandemic push for healthcare organizations to adopt more technologies and cloud applications and services, we've seen attackers keen on taking advantage of vulnerabilities and other security weaknesses to get access to protected health information (PHI) and personally identifiable information (PII) created, stored, received and transmitted by healthcare covered entities and business associates.

As healthcare adopts these solutions and technologies to keep up with rapidly changing consumer demands and service delivery models, attackers are identifying security gaps and taking full advantage, especially in the cloud.

So, what are some basic cloud security best practices that can help your organization keep patient data secure in the cloud?

First, it's important to understand that when it comes to cloud architecture and cloud environments there's no one-size-fits-all solution. What the cloud security model looks like for your organization depends on a number of specific and unique factors for your organization, such as your architecture. One cloud security framework that works for one organization may not be right for yours.

Some common influencing requirements to consider are:

- Data classification
- Specific configurations
- Access and privilege management
- Data security
- Data flow/orchestration

It's also helpful to understand that cloud data

security also has its own lifecycle: prevent, detect, respond, and remediate.

When we talk about cloud security best practices, think about:

- How can we prevent threat actors from accessing or exposing our data?
- Do we have enough processes and controls in place to detect incidents as they happen?
- What will we do when we detect an issue?
- How will we remediate those risks? For example, should we implement additional controls or sub-controls to prevent attempts?

Developing a Layered Approach for Cloud Security

In addition to tackling common issues such as misconfigurations and minimizing insider threats, when thinking about ways to keep patient data secure in the cloud, another best practice is to build a layered approach into your cloud security practices.

It might look something like this, starting at the bottom with your foundation and moving upward:

1. Foundational security: Conduct a security assessment of your cloud environment and begin cloud hardening
2. Technical testing: Conduct vulnerability assessments and technical testing, such as internal and external penetration tests to determine risks to your cloud environments
3. Monitoring and alerts: Identify misconfigurations and security events in your current environment
4. Secure cloud architecture: Conduct a maturity assessment for insight into your environment as it changes to ensure your controls function as designed and implement ongoing security risk management practices

Implementing Cloud Hardening

Another best practice to help keep your patient data safe in the cloud involves adopting cloud-hardening measures to secure your cloud environment.

If you haven't done so already, here are five recommended steps that may be helpful:

1. Conduct a security assessment.
2. Implement security controls based on policies, which are generally specific to your organization. There are a variety of policy templates your organization can draw from or you can create your own based on your organization's unique requirements.
3. Implement technical testing such as vulnerability testing and penetration tests.
4. Perform ongoing environment monitoring, maintenance and support.
5. Maintain secure architecture development practices and conduct ongoing cloud security review.

7 Best Practices for Cloud Security

1. **Implement a strong identity foundation:** Implement the principle of least privilege.
2. **Enable traceability:** Monitor, alert and audit actions and changes to your environment in real-time.
3. **Apply security at all layers:** Apply a defense in depth with multiple security controls.
4. **Automate security best practices:** Automated software-based security mechanisms improve an organization's ability to scale security.
5. **Protect data in transit and at rest:** Classify your data into sensitivity levels and use mechanisms, such as encryption, tokenization and access control where appropriate.
6. **Keep people away from data:** Use mechanisms and tools to reduce or eliminate the need for manual processing.
7. **Prepare for security events:** Prepare incident management and investigation policies and processes.

ALIGNING CLOUD SECURITY WITH YOUR BUSINESS STRATEGY

While adopting best practices and implementing industry recognized controls are important parts of your cloud security strategy, there's another important component that some security teams overlook—the value of aligning your cloud security program with your business strategy.

As we mentioned earlier, from cost savings to scalability, there are a number of good business reasons your healthcare organization may want to facilitate rapid cloud adoption across your enterprise. But those benefits also bring a range of risks to your organization. That's why it's important to also create and maintain a business-driven cloud strategy—one that's structured, yet agile-driven for optimal cloud services delivery.

What might that look like for your organization? Here are some considerations:

- Develop a cloud transformation strategy
- Understand your organization's business objectives
- Include application migration strategies
- Adopt a team-focused operating model
- Deploy automated solutions
- Engage enterprise governance
- Adopt Agile design and workflow
- Expand and scale teams
- Accelerate migration velocity and launch modernization

It's worth pausing a moment to expand a little more on the idea of a team-focused model to help align your cloud security program with your business objectives. It's not just about getting the doers, those responsible for related day-to-day tasks on board with your vision. It's about building a broad base of support for your program throughout the organization.

Often, that success is directly tied to building executive and key stakeholder engagement for your program, and that's why the concept of business strategy alignment is so important. Think of it as a way to speak about your cloud security goals, objectives and needs in a language your executives and board understand—in business terms.

It's always helpful to build engagement as early as possible. For example, seek out a C-suite level executive willing to sponsor and champion your program through the organization. This leader can play a key role in setting program goals as they relate to other critical business objectives.

Your sponsor also plays an important role in helping you communicate your program's value proposition broadly across the business to get more executive involvement and support of your initiatives. This can help create strong joint ownership of program outcomes that align closely with business goals. It's a way to tie your program directly to business enablement and helps you both measure and communicate progress and outcomes in a way key stakeholders understand.

Need assistance developing and implementing a strategy for ensuring the security of your data in the cloud?

Learn about Clearwater's capabilities here and contact us to discuss how we can help.