Clearwater

Whitepaper

Healthcare’s Cloud Migration

7 Emerging Data Security Challenges and How to Manage Them

ClearwaterSecurity.com

Healthcare—Secure, Compliant, Resilient

Table of Contents

Introduction

Healthcare in the cloud

Seeking flexibility, scalability, and cost-savings, an increasing number of healthcare organizations are moving systems and data to the Cloud. This trend appears to be accelerating, fueled by increased adoption of telemedicine and wearable medical devices sparked by the 2020 coronavirus pandemic and continuing investment and growth in cloud-native health IT startups.

In 2014, a survey shared in Forbes estimated that more than 80% of healthcare organizations were using cloud services, with almost 70% adopting SaaS-based applications.

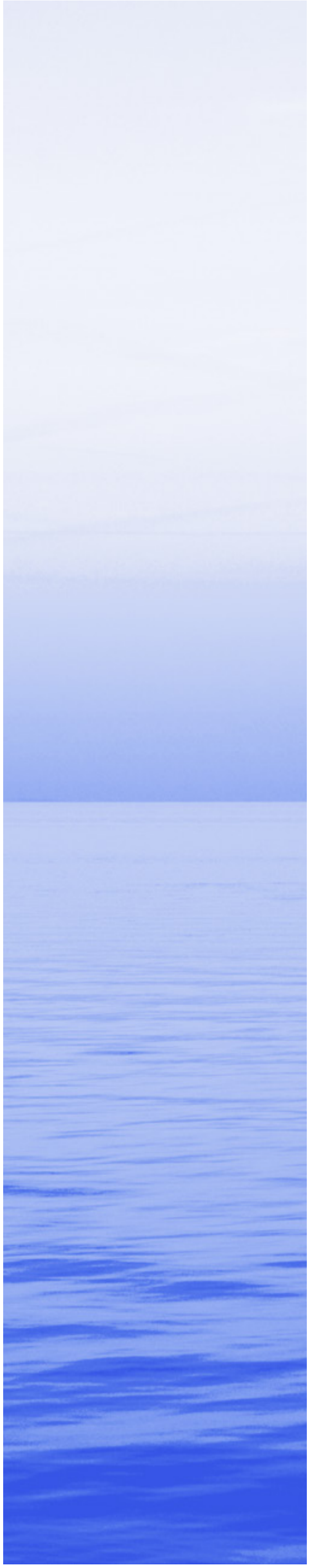
In a more recent 2019 study, this one from Netwrix, almost 75% of healthcare organizations said they store at least some healthcare and employee data in the Cloud, and 32% of healthcare respondents said they store sensitive data like personal health information (PHI) and personally identifiable information (PII) in the Cloud.

Based on trends we see with the pandemic response, especially the move across all industries to adopt more remote workforce capabilities, we can likely expect cloud adoption—in some form—to continue to increase going forward.

Today, the Nutanix Enterprise Cloud Index for healthcare finds that hybrid cloud models are thought by almost 87% of surveyed organizations to be the ideal deployment model, with more than 40% of healthcare respondents saying they intend to increase hybrid cloud usage in the next three-to-five years while decreasing traditional data center usage (33%).

That same survey indicated that security and regulation drive hybrid cloud adoption, with 33% of respondents stating they believe it is the most secure alternative, followed by on-prem private clouds as the second-most secure at 21%.

Interestingly, while many industries rely at least in part on public clouds for operations, in this survey, just 7% of healthcare entities say it is the most secure option for their organization.



What is the 'cloud?'

For many users, the term "the Cloud" is abstract, often even ambiguous, encompassing every IT system or asset accessed off-site through the Internet.

Here's how the National Institute of Standards and Technology (NIST) defines cloud computing: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

But what does that actually mean? What is the Cloud?

The best place to start is with three key concepts. These are abstraction, virtualization, and orchestration. Understanding these concepts is foundational to understand the Cloud. Let's take a look at each.

Abstraction may be thought of as only providing what is essential and concealing the rest. In a cloud service, the cloud service provider (CSP) only delivers to the customer the information and capability they need for their use. The complexity and detail that allows the CSP to provide the services are hidden from the customer and managed by the CSP. The layer at which the abstraction takes place defines the service model of a cloud service. We will talk more about service levels shortly.

Virtualization is the replication of what is typically thought of as tangible IT assets using software. For example, traditionally if I wanted to set up a server, I would first obtain hardware (the physical computer) and install the operating system and server software, plug it into the network and fire it up. In the Cloud, I can create that server's virtual equivalent by merely making a few clicks and a few configuration decisions. Using virtualization allows a CSP to have many virtual servers running on one traditional server.

When a CSP provides a cloud environment on top of the traditional infrastructure, many potential benefits emerge. When combined with orchestration, that potential is realized both by the CSP and its customers. Abstraction and virtualization allow the CSP to create virtual computing resources and offer them to customers. Orchestration provides the ability to pool and efficiently manage these resources while delivering them to customers on-demand. Using segregation, the CSP can make the resources available to customers through the Internet and share the resources across multiple tenants, increasing efficiency, and reducing cost.

As mentioned above, the abstraction layer defines the Cloud service model the CSP is offering. Each cloud service model describes the services provided to the customer. Everything needed to support the service delivery below the layer of abstraction is the CSP’s responsibility. The service models include:

Infrastructure as a Service – CSP offers customer access to a resource pool of fundamental computing infrastructure. This model is similar to a virtual data center with virtual compute, network, and storage available to the customer.

Platform as a Service – CSP abstracts the underlying servers, networks, and infrastructure providing customers with development or application platforms or capability upon which they can build and manage applications.

Software as a Service – CSP manages and provides a full application that customers access through a browser or lightweight client application.

Cloud deployment options

There are four primary cloud deployment models: public, private, hybrid, and community.

When most people think of the Cloud, they think of a public cloud model like Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP). These are public hosting services, many of us use daily—for example, to save files on Google Drive or store photos from your cellphone.

Then there is a private cloud set up for one user (or entity) and accessed through a private network.

Lesser known is the community cloud, which is similar to a public cloud. Still, instead of having the pool of resources accessed by anyone, it is generally set up for related communities where the Cloud is accessible to a specific community or group, but not to the entire public.

Finally, there is a hybrid cloud model, and when people refer to a hybrid cloud, they may refer to one of two options:

1. Use of a mix of public cloud and private cloud solutions
2. Use of either a public or private cloud (or both) and on-premises solutions

Cloud benefit

Why are more healthcare entities moving their data and services to the Cloud? Here are three frequently cited reasons:

1. **Scalability:** The Cloud offers scalability and flexibility in deploying assets.
2. **Cost:** A cloud model enables healthcare entities to pay for only those resources they need at any given time, often offering increased cost-savings.
3. **Security:** Is the Cloud more secure? The best answer is it depends. In light of increases in successful cloud-based data breaches, especially in shared (public or community) cloud models, some organizations are considering a move back to on-premises hosting to retain more control over data security.

Cloud risks

While there are increasing benefits for healthcare organizations that adopt cloud models, introducing sensitive and protected data into the Cloud creates various new risks. As we've seen in some surveys, organizations are conflicted on whether cloud security makes it easier or more challenging to manage these risks.

We believe the answer is, it depends. Suppose an organization has the expertise to understand the Cloud's unique security risks and how to appropriately leverage the many safeguards available from the more reputable CSPs. In that case, they will be able to manage the risk effectively. If organizations don't have the expertise, the complexity and difference of the Cloud mean risks can quickly turn into a reality with significant impacts on organizations, partners, and patients.

Netwrix's survey indicated that almost 40% of respondents had a cloud security incident in the previous year, and nearly half of them could not diagnose the issue.

> Cloud creates various new risks. As we've seen in some surveys, organizations are conflicted on whether cloud security makes it easier or more challenging to manage these risks.

Understanding cloud security

One complexity of cloud security is that unlike traditional on-prem assets where security responsibility falls solely within your organization (or a third-party if you outsource it), cloud security is a shared security model. Some of the responsibility for cloud security belongs to the CSP, while other components are the customer's responsibility.

Where the responsibilities delineate depends on the service model and the CSP. For example, in an IaaS model, the CSP typically has security responsibility for the facilities, infrastructure, and network that supports the infrastructure. In a PaaS model, in addition to the IaaS responsibilities, the CSP typically manages all network controls and some application-level controls. In the SaaS model, the CSP typically also manages application controls and some of the identity and access management controls. While this generally describes the responsibilities, there are differences between CSPs, and customers must understand precisely where the CSP's security responsibilities stop and theirs begins.

When it comes to cloud security, it is important to point out here that while a customer transfers some security responsibility to the CSP through the shared security model, they cannot transfer their compliance responsibilities. For example, suppose electronic protected health information flows to the CSP or CSP-supported resources. In that case, the customer is responsible for ensuring the CSP meets HIPAA compliance standards, and a Business Associate Agreement is in place.

Buckets of trouble

If you're keeping your eye on cybersecurity trends this year, you've likely heard about the significant data breach that originated with Blackbaud. This cloud computing provider services a gamut of industries, including higher education, healthcare, and nonprofits.

What began as a ransomware attack ended up in data exfiltration, compromising hundreds of thousands of records. The affected organizations represent just some of the almost 450 healthcare organizations that have reported a data breach so far in 2020 (of 500 or more records per breach) and who the Office for Civil Rights (OCR) is now investigating.

And while these successful breaches make big headlines, they represent only a fraction of the potential exposures that can exist in cloud environments because of vulnerabilities, misconfigurations, and other undetected security issues.

For example, in August of this year, a researcher discovered a misconfiguration issue for a healthcare entity using Amazon Simple Storage Service (Amazon S3), a private cloud storage solution. With Amazon S3, users can store data and then restrict access to ensure it is only accessible by specific, authorized users.

However, if a customer does not appropriately configure the Amazon S3 bucket, anyone with Internet access can access the data.

Unfortunately, this is one of many that shows an emerging pattern of risk created by improperly configured clouds—whether public or private.

Why is this happening?

Well, it is rooted in one of those benefits of cloud adoption. While cloud solutions can be straightforward to set up and use (often just a few mouse clicks to get you on your way), they can be complicated—without the right experience and knowledge—to configure correctly and maintain. This concern is especially relevant when customers are unclear about who is responsible for which security processes and procedures.

August 2

Researchers contact DataBreach.net to say they discovered a misconfigured Amazon S3 bucket with 61,000 medical records.

August 3

DataBreach.net and researchers contract BioTel and SplashRx as potential owners of the bucket. The researchers had access to scanned faxes with medical information about BioTel patients, which had been handled by SplashRX/HealthSplash.

August 5

Researchers and DataBreach.net again reached out to BioTel and SplashRx and got no response.

August 8

Researchers contacted the Amazon Abuse team to notify them of the bucket issue and ask Amazon to notify the bucket’s owners.

August 9

Bucket locked down.

November 1

No evidence of either entity reporting this as a breach or of any other entity reporting this incident to OCR.

Seven emerging security challenges in the cloud

When it comes to cloud security, if you want to keep your data in the Cloud, or begin the migration of systems and applications to the Cloud, where should you focus your attention? Let's look at seven emerging challenges to maintaining security in the Cloud and recommendations on how to address these challenges:

Security Challenge	Recommendations
1. Containers/Virtual Machines (VM) *Security Concern: Insecure Configurations* While containers and virtual machines are easy to set up and use, if developers don't secure them or configure them properly, then the containers and contents (data) can be discovered and accessed by bad actors (using specialized search tools like Shodan).	1. Maintain a current inventory of assets 2. Implement and enforce configuration management policies and procedures 3. Automate configuration and security checks, including DevOps and OpSec 4. Leverage native tools like AWS Security Hub and Azure Security Center 5. Test regularly and use tools like Shodan to see what others see
2. Multi-Factor Authentication (MFA) *Security Concern: Identity and Access Control* If you're using single-factor authentication and a bad actor compromises a user's credentials, the attacker can gain access to all resources the user can access, which can result in data exfiltration, ransomware, or other malicious acts.	1. Determine your MFA goals 2. Determine the best solution to meet your goals (every time, certain situations, risk-based) 3. Implement the solution
3. Keeping Secrets Secret *Security Concern: Managing Secrets, Keys, Certificates* If you don't manage and secure your keys, secrets, certificates, etc. (or they're hardcoded in software), an attacker can access everything it unlocks.	1. Find and remove any hard-coded keys 2. Implement policy and procedures to prevent hard coding 3. Change hard-coded keys 4. Implement secure key management solution (Secrets Manager, Key Vault) 5. Manage secrets on an ongoing basis 6. Limit root access

> If a customer does not appropriately configure the Amazon S3 bucket, anyone with Internet access can access the data.

Security Challenge	Recommendations
4. Encryption *Security Concern: Encrypting Data* If data at rest or in motion is not encrypted and an intruder gets access to a virtual machine or your network, the attacker can read that data. Since it can take, on average, hundreds of days for organizations to discover some data breaches, the attacker can see everything that’s passing through unencrypted and can make lateral moves across your network to access more data and systems.	1. Apply disk encryption to virtual machines 2. Secure access from on-prem to Cloud (VPN)
5. Web Application Firewall *Security Concern: Web Attacks* Web applications often have flaws in software like SQL injection and cross-site scripting. When attackers exploit these weaknesses, they can access the application and data.	1. Develop requirements 2. Consider managed or unmanaged 3. Identify vendors 4. Evaluate vendors 5. Select vendor
6. Logging *Security Concern: Lack of Logs or Log Review* If you do not keep or review logs, you may not be able to identify when you have a breach of if threat actors are actively engaging in malicious activities, which puts your data at risk for ongoing exfiltration.	1. Turn on event logging 2. Establish policy and procedures 3. Regularly review logs 4. Consider an investment in a system information and event management (SIEM) solution

Security Challenge	Recommendations
7. Patching/Software Updates *Security Concern: Unpatched, Deprecated, Unsupported Software* Most software, applications, and operating systems (OS) have vulnerabilities. When developers identify these issues, they'll often release patches or updates to correct the security risks. If you do not (or can't) apply the patch or update, the software remains vulnerable to attacks. Just like your on-prem assets, if you're deploying virtual machines or other software and applications in a shared responsibility security model, you'll need to ensure they're patched and updated. When they can't be (for example, it may affect functionality or create disruptions or downtime), you'll need to apply compensating controls to mitigate your risks until you can apply the patch. Remember, the longer a vulnerability is unpatched, the more likely it is that an attacker will attempt to exploit it.	1. Create and maintain an inventory of software 2. Prioritize systems/software 3. Develop and implement patch management policies and procedures 4. Monitor vendors for patch updates 5. Test before applying a patch 6. Apply compensating controls until patches applied 7. Apply a patch as soon as possible

General cloud security recommendations

While the emerging security concerns above are prevalent in Cloud environments, there are general best practices you can adopt to ensure your Clouds remain secure, no matter what the next significant threat may be.

To keep your public, private, hybrid, or community Cloud environment safe, it's essential to:

1. Understand your shared security responsibilities
2. Understand the environment because it will influence your security measures
3. Classify all information because not all information requires the same security controls
4. Implement baseline controls (suggestions: NIST, CSA, CIS, FedRAMP, and other regulatory and compliance-based measures)
5. Perform risk management, including risk analysis:

   a. What's your level of acceptable risk?

   b. What's your risk threshold?

   c. What do you do when an issue exceeds your level of acceptable risk?

6. Test controls to ensure they're functioning as you intended

7. Monitor systems to make sure that your controls are effective and protecting the confidentiality, integrity, and availability of your data

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact