HOW TO DEPLOY A SECURE CLOUD FOR HEALTHCARE

A GUIDE FOR DEPLOYING A COMPLIANT CLOUD

TALK TO AN EXPERT

EXECUTIVE SUMMARY

Cloud services offer clear benefits—performance, cost savings, and scalability to name a few—so it's no wonder healthcare organizations are eager to take advantage of all that the cloud has to offer. Unfortunately, vulnerabilities are often introduced to your network when you adopt new technology. Cloud computing is a prime example, as the implementation process brings security and compliance concerns.

HIPAA and HITRUST compliance adds an additional layer of complexity to cloud deployments, and consequently, you must be methodical about choosing the right cloud solution. Not to mention, effective security goes beyond compliance standards; mandated compliance measures are the minimum. It's highly recommended to implement additional security measures on top of the compliance standards to protect your sensitive data to the fullest.

Let's discuss how to identify and overcome common challenges in secure cloud deployments, so you can opportunistically adopt cloud-based solutions while remaining on the right side of the law.

STATE OF THE CLOUD

According to the HIMSS 2023 Survey, 88 percent of providers are currently using a cloud service. This data suggests that security and compliance concerns do not appear to be major obstacles for organizations in deploying cloud environments. Despite this increased adoption, the number of breaches and security issues continues to rise, highlighting potential inadequacies in the development and management of cloud deployments.

Healthcare has consistently ranked as one of the top industries with the highest number of cybersecurity breaches since 2005. Multiple factors contribute to these breaches and compliance violations, and the consequences have become more severe, with the cost of a breach continuing to escalate. Healthcare remains a prime target for cyberattacks. In 2016 alone, **a staggering 1 million healthcare records were exposed**, and the average cost of a data breach reached $2.2 million.

TOP CHALLENGES IN DEPLOYMENT

The first step in overcoming your challenges is to identify them and understand their impact. These challenges affect different departments within your organization, as cloud adoption requires alignment across your business, operations, and technical teams. Let's dive into each one to better understand how they affect your day-to-day operations.

Ambiguous Delegation of Responsibilities

When technology is new to an organization, the responsibility of finding and managing that solution is often unclear. You must determine who owns your data. Is it your IT Department? Or perhaps your Security Department? It's difficult to coordinate different people across departments, and even more difficult to communicate effectively between your organization and your provider. The delegation of responsibilities between you and your business associate will vary based on your service model, i.e. software as a service, infrastructure as a service, etc.

Lack of Data Governance

If you don't have a solid foundation of policies, standards, and practices, your organization is creating vulnerabilities. Common issues include:

- Shadow IT: According to a recent survey, 40% of cloud services are commissioned without IT input.
- 2 Portability and Mobility: Mitigating risks among many endpoints has become more challenging with bringing your own mobile device (BYOD), wearables, and other smart devices connected to your network.
- Privileged User Access: You should minimize access as much as possible by dividing user access by work role.

> "NOT USING CLOUD IS NOT AN OPTION IF YOU WANT YOUR ORGANIZATION TO BE SUCCESSFUL TODAY AND IN THE FUTURE"
>
> - JIM MASTERSON, LIGHTEDGE CEO

Safeguarding Data & Meeting Required Controls

The HIPAA Privacy Rule, the HIPAA Security Rule, and HITECH combined protect ePHI and establish the national standards. Your concern is the confidentiality, availability, and integrity of sensitive data. In practice, this includes:

- Technology
- Safeguards (Physical & Administrative)
- Process
- People
- Business Associates & Support
- Auditable Compliance (Proving Your Compliance)

As you can see, there are many moving parts. Do you feel prepared for an audit if it happened tomorrow?

Ensuring Data Availability, Reliability, & Integrity

The key to service reliability and uptime is in your data backups and disaster recovery (DR) efforts. Data backup is not the same as disaster recovery—this is a common misconception. Data backup is part of business continuity planning, but requires much more.

According to the latest *CloudEndure* survey conducted in 2023, there remains a significant disparity between how organizations perceive their track records and the actual state of their Disaster Recovery (DR) capabilities. The survey indicates that 85% of respondents believe they meet their availability goals, but only 42% consistently achieve these targets. Alarmingly, 28% of the organizations surveyed do not have a system in place to measure service availability. It's important to note that downtime can still occur due to factors beyond an organization's control, including issues with their cloud providers. For example, a recent AWS outage caused widespread disruptions when numerous cloud-based services ceased to function. In the past three months, 62% of organizations reported experiencing at least one outage event. This highlights the ongoing challenges in maintaining high availability and the need for improved disaster recovery strategies.

The ability to convey auditable compliance (transparency) investors, customers, and regulators cannot easily discern that your cloud environment is compliant because it's not as visible as other solutions, like on-premise hosting. You will have to work closely with your cloud provider to identify how to document your technology, policies, and procedures in order to document your efforts and prove auditable compliance.

UNDERSTANDING CLOUD CRITERIA

There are many types of cloud models, from public to private and everything in between, each with their own features and levels of security. Selecting among the many available options is confusing and frustrating—use the following criteria to find the right solution(s):

Assess the Risks

- What level of data protection do you require? How your data is classified and how it's used and/or accessed will determine the level of risk you're willing to accept.
- What if the asset became public information?
- How would you be harmed if an outsider manipulated a process or function?
- How would you be harmed if the data were unavailable for a period of time?

****Warning: Data availability is flexible, but confidentiality is not!****

For example, medical records are critical during emergency treatments. The same patient information is necessary for billing, but only accessed once a month. Even though your availability needs differ for the same information, the confidentiality of the data does not change.

Determine Workload Performance

You can use a private cloud for your health information exchange and deploy a separate cloud environment for your back-office applications. Efficient configurations often end up in a hybrid cloud approach—when you use only what you need, you are minimizing costs.

Choose the Proper Audit Assessments

Some providers restrict vulnerability and penetration testing, while others limit the availability of audit logs and activity monitoring. Find a solution with a provider that's aligned with your risk management requirements.

BEST PRACTICES

With an understanding of your organization's cloud criteria, you are better equipped to act. There's a plethora of sources advising how to stay secure and compliant in the cloud, but there are only a few sources that are trustworthy:

- NIST Publications (800-145, 800-66, 800-52)
- Office for Civil Rights (OCR)
- U.S. Department of Health & Human Services (HHS)
- Cloud Council
- Security Rule Educational Series
- Breach Notification Rule

These trusted sources note what technology is required, and which are addressable—meaning, applicable to your organization. Just because a control is addressable does not mean it's optional. You should follow both the required and addressable security measures.

The number one mistake organizations make in cloud deployment is INSUFFICIENT ENCRYPTION. Encryption must be FIPS 150-2 compliant.

The number-one mistake organizations make in cloud deployments is insufficient encryption, followed by key management. Encryption must be FIPS 140-2 compliant.

The National Institute of Standards and Technology (NIST) produced the FIPS publication series to help you with best practices. FIPS 140-2 "Security Requirements for Cryptographic Modules" covers the design and implementation of a cryptographic module (i.e. hardware, firmware, and software that implements cryptographic functions like encryption and decryption).

Seek the Right Technology

As previously mentioned, you should seek technology solutions and controls that are both required and addressed. When it comes to security, you can never be too prepared. Here are some of the technology measures you'll want to implement:

- Data Encryption in Transit and at Rest
- Firewalls
- Multi-Factor Authentication
- Cloud Encryption Key Management
- Audit Logs Showing Access to ePHI
- Vulnerability Scanning, Intrusion Detection/Prevention
- Hardware and OS Patching
- Security Audits
- Contingency Planning: Regular BU/DR Plan

Select a Secure Cloud Provider

Remember when selecting your cloud provider(s) is that you must ensure auditable compliance and that security responsibilities are shared. We discussed the idea of transparency earlier, and it cannot be stressed enough. Your provider should have the proper credentials, satisfy your required technical and administrative safeguards, and meet your service level agreement (SLA) terms, as well as, your business associated agreement (BAA) needs.

Look for provider credentials and security levels, such as ISO, SOC, HIPAA, and PCI. These standards demonstrate that a third-party has audited their facilities to verify their status for compliance.

SLAs and Business Associate Agreement Terms Start with the OCR's sample BAA and customize to fit your organization. Develop defined roles and responsibilities (per HITECH Act of 2009) with limited privileged access. Terms should include:

- Outlined policies, procedures, and reporting (such as security incident response procedures and data decommissioning at the end of the contract)
- Guaranteed response times in SLA

CONCLUSION

The cloud provides significant advantages, from cost savings to flexibility, but transitioning into the cloud requires a thorough road map with checkpoints for security and compliance along the way. You'll want to identify internal resources from IT, security, and operations to participate in your cloud deployment process. Use our cloud criteria and best practices to evaluate and select a cloud service provider.

ABOUT LIGHTEDGE

LightEdge offers HIPAA compliant data center services with a focus on delivering highly available and secure hybrid hosting. Their solutions help organizations meet the most rigorous compliance standards including, HIPAA, HITRUST, PCI, SOC, ISO, and NIST.

LightEdge has one of the strongest compliance and security solutions portfolios on the market. They operate seven enterprise-class data centers to deploy cloud computing, colocation, disaster recovery, and managed services all wrapped in 24/7/365 expert support.