Clearwater

Whitepaper

Understanding Azure Basics: How to Ensure HIPAA Security and Compliance in a Cloud Environment

Table of Contents

Introduction 3

Risks and challenges of the cloud 4

Third-party risk 5

Best practices to reduce risk 6

The shared responsibility model 7

Breach reporting 9

More on Azure best practices 9

Architecting a cloud solution 9

Should you move to the cloud? 10

Adopting and maintaining a lifecycle approach 10

Key takeaways 11

© Clearwater | All Rights Reserved | WP-36.2

Introduction

A growing number of healthcare organizations are realizing the benefits of moving to the cloud.

In Q3 of 2022, global cloud infrastructure spending hit $57 billion, bringing the industry total for the previous 12 months to $217 billion. This number is expected to climb to $519 billion by 2027, demonstrating meaningful interest and investment in cloud environments for healthcare and other industries.

85% of organizations are expected to embrace a principle by 2025, a trend reflected in healthcare for covered entities and business associates.

There are several cloud service providers (CSPs) well-equipped to handle healthcare cloud migration needs, for example, Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Services (GCS).

Many healthcare organizations use Microsoft services on-prem. These organizations often choose to move into the cloud with Azure because of their familiarity with the Microsoft environment. It's estimated that Azure controls about 21% of the cloud infrastructure market today.

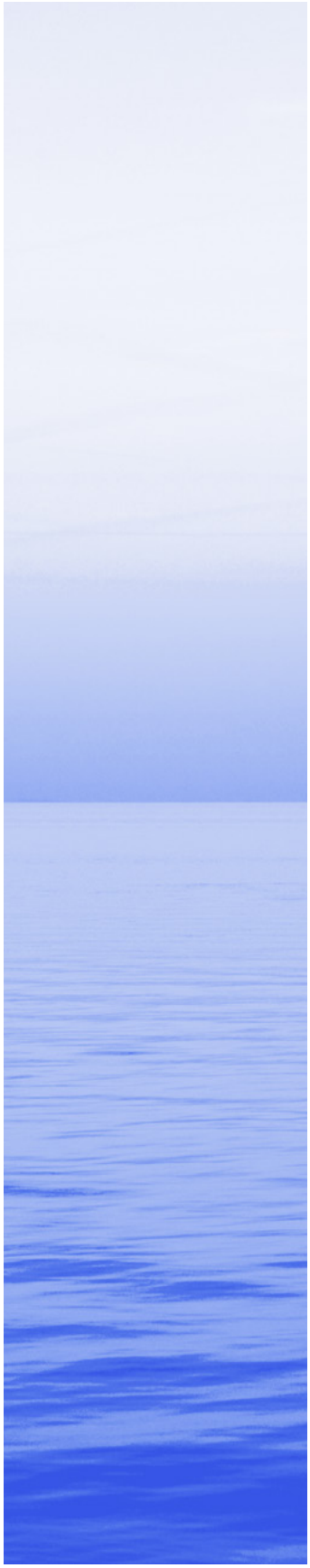
Across the industry, we're seeing hospitals, integrated delivery networks (IDNs), and their digital health partners adopting measures to improve care delivery with Azure. Microsoft even provides a list of solution ideas for using Azure to support healthcare.

While shifting to the cloud may make sense from a technical and business standpoint, moving to the cloud introduces complexities and new risks related to electronic protected health information (ePHI) and compliance with the HIPAA Security Rule.

When done properly, moving into a cloud-only or hybrid on-prem/cloud environment is generally safe; it's important to note that adopting a CSPs like Azure does not automatically make your organization secure or HIPAA compliant.

So, as a healthcare provider or business associate, from a security and compliance perspective, what do you need to do to ensure your cloud environment meets HIPAA standards?

In this white paper, we take a closer look at the shift into the cloud, what that means for security and compliance, and offer tips on what your organization can do to get the most out of Azure without putting patient health data at risk.



© Clearwater | All Rights Reserved | WP-36.2

Risks and challenges of the cloud

As mentioned above, moving to the cloud, whether in a SaaS, PaaS, or IaaS model is not inherently riskier than a traditional on-premises model. Where issues often occur is when there is a misconfiguration of cloud assets. Unlike a misconfiguration in an on-prem situation that may only expose the asset within the on-prem network, a misconfiguration in the cloud will often expose the asset to the world.

For example, in 2019, a pair of researchers discovered an unsecured cloud server hosted on Azure, which provided access to a database containing 24GB of unencrypted data on 80 million U.S. households. That data included names, addresses, income brackets, marital status, birthdates, and exact location information.

While details about whom the server belongs to were not made public, researchers suggested it could have been an insurance, healthcare, or mortgage company. After the researchers notified Microsoft about the server, that database was publicly unavailable.

In 2020, researchers contacted DataBreach.net informing them that a misconfigured Amazon S3 Bucket contained 61,000 medical records, which they later identified as likely belonging to BioTel and SplashRx.

The researchers reached out to these two organizations but got no response, so eventually, they connected directly with Amazon, and as a result, the bucket was locked down.

While risks and challenges are unique for every organization, some common areas that often plague organizations of all sizes include the following:

- Not knowing what HIPAA or Azure requires for security and compliance
- Inability to attract and retain enough skilled cloud engineers
- Not reviewing monitoring processes or logs

While breaches and record exposures continue to increase, there are some lessons we can draw from what's happening in the world around us.

First, among the benefits of the cloud, it enables the ability to grant anyone access to cloud resources from anywhere with an Internet connection. This is unlike traditional on-prem networks, where controlling access to internal resources is a bit less complex and misconfigurations, in turn, are typically a bit less risky.

Cloud environments are complex, and so are their configurations. That complexity can lead to security and compliance holes, even for organizations that use industry-recognized controls and frameworks.

© Clearwater | All Rights Reserved | WP-36.2

It's not uncommon to discover cloud breaches where:

- Networking restrictions and Identity and Access Management (IAM) controls were not in place
- Developers architected a system or application for convenience but did not include security from day one.

Unfortunately, security is often an afterthought in design and development processes, but healthcare organizations should focus more on changing that mindset. The risks are too great, especially in the cloud.

To circumvent these issues, be intentional about what your security and compliance processes look like and ensure they're built into your system development lifecycle (SDLC).

In addition to those challenges, shadow cloud IT remains a concern. This is probably an even bigger problem in the cloud because it's easier for developers to spin up new things within the cloud, posing unique and specific security challenges for your entire organization.

Third-party risk

Of course, moving to the cloud does not necessarily mean that an organization will be building or hosting its services. Almost every cloud strategy involves using partners in the form of CSPs, PaaS, and SaaS providers.

While there are still individuals in the industry who are under the misperception that moving to the cloud immediately implies that they are HIPAA compliant and secure, most healthcare organizations now realize it is not quite that simple. Healthcare providers adopting cloud services are increasingly interested in ensuring their service providers are HIPAA-compliant and secure.

Requiring service providers to enter into business associate agreements when appropriate is required under the HIPAA Security Rule, and requiring that they provide information on their security program on an ongoing basis to help their customers understand their risk is now the norm.

© Clearwater | All Rights Reserved | WP-36.2

Best practices to reduce risk

So, what can you do to address Azure security and HIPAA compliance? Here are some best practices to consider.

One of the best places to start is with the security best practices offered by your cloud services provider.

Most big CSPs, like Azure and AWS, have various resources available for those using their cloud services. For example, Azure's best security practices are accessible on its website.

Why is this a good place to start? The cloud security practices shared by the CSP generally align directly with the functionality and naming convention of the provider itself.

Consider zero trust. With zero trust, we assume that even with the best controls, a threat actor may still breach our defenses.

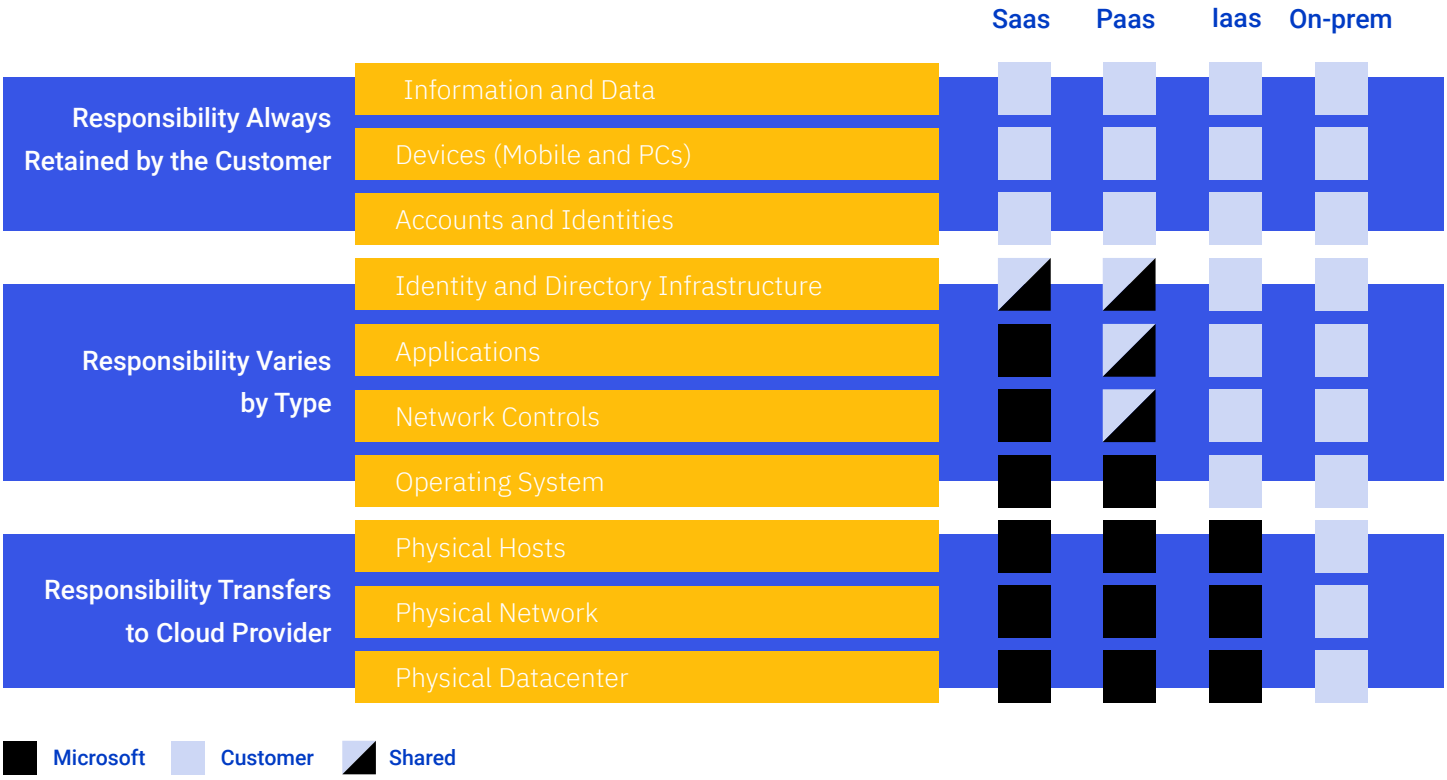
For example, Azure's zero trust best practice is to give conditional access to resources based on device, identity, assurance, network location, and more.

But the Azure recommendations go even further—the recommendation says that Azure Active Directory (AD) conditional access will enable you to apply access controls by implementing automated access control decisions based on required conditions.

Another Azure best practice is to enable port access only after workflow approval. To do that, the recommendation indicates you can use just-in-time VM access in Microsoft Defender for Cloud to lock down inbound traffic to your Azure VMs. That should reduce attack exposure while providing easy access to connect to VMs as needed.

One more best practice—grant temporary permissions to perform privileged tasks to prevent malicious or unauthorized users from gaining access after permissions expire. Access is granted only when users need it. To do that in Azure, use just-in-time access in Azure AD Privileged Identity Management or a third-party solution to grant permissions to perform privileged tasks.

© Clearwater | All Rights Reserved | WP-36.2



The shared responsibility model

While these are solid starting points for Azure, it's still important to remember that utilizing Azure best practices does not guarantee that you're HIPAA compliant.

While you can use Azure to process ePHI, you're still responsible for ensuring your organization and all business associates that create, receive, store, or transmit ePHI on your organization's behalf are HIPAA compliant.

It's helpful that Azure handles many cloud security components; however, as the healthcare covered entity, cloud security for your ePHI is ultimately your responsibility. You can't completely hand off responsibility to the CSP. Instead, you should think of it in terms of a shared responsibility model.

In a shared responsibility model, you and the CSP have specific security elements for which you're responsible. No third-party CSP will take full responsibility for all things cloud security. Here are a few examples of what shared responsibility might look like in an Azure environment.

© Clearwater | All Rights Reserved | WP-36.2

It's also important to understand that systems are not HIPAA compliant; organizations are. For your organization to be HIPAA compliant, you must employ certain security safeguards in your systems and environment.

As a HIPAA covered entity or business associate you must:

- Ensure the confidentiality, integrity, and availability of ePHI
- Identify and protect against reasonably anticipated threats to the security or integrity of the information
- Protect against reasonably anticipated, impermissible uses or disclosures
- Ensure compliance by your workforce

The HIPAA Security Rule also requires specific baseline controls to be in place. There are both required safeguards and addressable safeguards. Required safeguards are fairly self-explanatory; however, addressable safeguards are not optional. Addressable safeguards are the controls that, if you don't implement them, you must explain and document why you don't and what you're doing to address those issues. This includes administrative, technical, and physical controls under the Security Rule.

A closer look at these control types, both required and addressable:

- There are also organizational controls such as:
- Business associate agreements must comply with applicable requirements
- Covered entities must report incidents and breaches
- Flow HIPAA requirements to subcontractors

The biggest takeaway is that your organization is ultimately responsible for protecting all ePHI.

Azure will agree to process ePHI if you comply with its business associate agreement. The agreement is enabled by default for all customers. There is no need to sign; however, having an agreement with Microsoft doesn't mean you are HIPAA compliant only that you have met the requirements for the business associate agreement.

The agreement indicates Microsoft is responsible for requirements on their end, but your organization is responsible for your requirements based on that shared responsibility model.

- You must only use Azure services that are in scope for you
- Microsoft makes contractual assurances
- Third-party audits and assessments are downloadable

© Clearwater | All Rights Reserved | WP-36.2

Breach reporting

Ultimately, the responsibility for protecting ePHI resides with the organization that originally collected the ePHI. So, business associates typically report a breach to their providers, but it's the provider's responsibility to ultimately report to OCR and notify impacted individuals and the press if required.

Remember, your organization can't transfer responsibility for ePHI protection to a third party. You can transfer responsibility for some of the controls, and you will do that through a shared security model and a business associate agreement. Ultimately, at the end of the day, don't lose track of your responsibilities.

More on Azure best practices

Azure does a good job recommending best practices; however, it's not a one-size-fits-all model. The Azure Built-In Initiative, for example, helps assess compliance but does not guarantee it. There are also regulatory compliance requirements beyond HIPAA, which can depend on various factors, including your location and the services you offer.

Architecting a cloud solution

Organizations building compliance and security programs for cloud environments commonly ask, "Where do we begin?"

There are a lot of different elements in play; here are some key areas to think about right out of the gate:

- Azure AD tenant design
- Subscriptions and resource groups
- Network segmentation to reduce the potential impact
- Data storage
  - How will you store your data if you have a breach?
  - What type of encryption will we use?
- Workloads
- Connections into and out of your network
- Anti-malware

© Clearwater | All Rights Reserved | WP-36.2

- Monitoring logging on an ongoing basis
- Planning for high availability, disaster recovery, and backup/restore

Often organizations build first and think about security and compliance second, but this can set your organization up for failure.

It can be more challenging and expensive to architect your security and compliance controls after a solution is developed than at the beginning. It is typically even more expensive and time-consuming to address these areas after your team has implemented your cloud solution. So, develop processes where security and compliance are a way of doing business daily within your organization and encourage these issues to be addressed as early as possible.

Should you move to the cloud?

While many healthcare organizations already understand the scalability, flexibility, and cost-savings benefits of cloud adoption, you may still be considering which is best for your organization: on-prem, in the cloud, or a hybrid model. There are positives and negatives to each of these and which is best depends on factors unique to your organization.

Regardless of which option you choose, approach your security and compliance programs from that zero-trust perspective, build the best defenses you can to prevent a breach, and be prepared to quickly discover a breach if one happens so you can respond, recover, and resume normal operations as soon as possible with the least amount of negative impact.

Be sure to encrypt everything you can, and also consider:

- Protecting and retaining logs
- Adopting infrastructure-as-code
- Understanding that automation is a two-edged sword

Adopting and maintaining a lifecycle approach

What can you do to ensure your security and compliance processes are always front-of-mind for all your team members?

Develop a culture that's well-versed in adopting and maintaining a lifecycle approach with everything you do. That means considering compliance and security throughout the entire lifecycle, especially as new components spin up within your environment.

© Clearwater | All Rights Reserved | WP-36.2

Here are some helpful recommendations:

- Plan - Utilize Azure best practices
- Assess - Understand the risk for all ePHI processed within your environment
- Build - Build a solution that meets compliance requirements and addresses risk
- Test - Test your cloud security regularly to identify vulnerabilities
- Run - Monitor cloud security on an ongoing basis to detect and respond to incidents

Key takeaways

The cloud can be a safe environment for healthcare organizations, and utilizing a CSP like Azure may bring your organization additional benefits not available from hosting everything on-prem.

Remember, you can never turn a blind eye to security and compliance requirements nor shift full responsibility for security and compliance to your CSP. As a covered entity, you're ultimately responsible for ensuring the confidentiality, integrity, and availability of your ePHI. If you are a business associate, you are contractually obligated and legally obligated to meet your obligations under the business associate agreement and the HIPAA Security Rule.

You can build organizational confidence in your security and compliance measures by:

- Adopting best practices for your CSP
- Building security and compliance into your processes from the start
- Routinely conducting tests and exercises to ensure the controls you have in place function as intended
- Discovering and remediating vulnerabilities, misconfiguration, and other security issues on an ongoing basis
- Adopting and employing routine risk analysis and risk management processes.

© Clearwater | All Rights Reserved | WP-36.2

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

© Clearwater | All Rights Reserved | WP-36.2