

cloudticity

Achieving HIPAA Compliance on Microsoft Azure: 10 Best Practices

Table of Contents

The need for HIPAA and HITRUST in public clouds 3

Establishing a HIPAA-compliant, HITRUST-certified environment on Azure 5

Implement key HIPAA/HITRUST best practices 6

- 1. Install multi-factor authentication 6
- 2. Configure platform logs 7
- 3. Fortify your business continuity strategy 8
- 4. Back up your data 9
- 5. Strengthen network and storage security – avoid default settings 10
- 6. Encrypt your data 11
- 7. Use robust, role-based access control 12
- 8. Sign up for Azure Active Directory Premium 13
- 9. Review Azure Security Center frequently 14
- 10. Conduct regular comprehensive reviews 15

Maintain HIPAA compliance and HITRUST certification with Cloudticity Oxygen 16

Get Started 18

The need for HIPAA and HITRUST in public clouds

Healthcare organizations are increasingly migrating to the cloud. They are using public cloud services to host patient-facing apps, generate new clinical and operational insights, facilitate collaboration among healthcare teams, and store fast-growing volumes of health data.

Public clouds give organizations the flexibility to rapidly scale resources while avoiding large capital expenditures. At the same time, today's leading public cloud providers can offer innovative technologies, such as artificial intelligence (AI) and analytics capabilities, which organizations can use to augment their services.

No matter how your healthcare organization uses the cloud, maintaining HIPAA compliance must be a top priority. You need to ensure the privacy and security of protected health information (PHI), safeguarding it from theft, fraud, and other unauthorized use. And you must be able to prove HIPAA compliance to regulators as well as patients and healthcare partners.



Many organizations use HITRUST Common Security Framework (CSF) certification as a way to demonstrate HIPAA compliance.

What are HIPAA and HITRUST?

HIPAA (the Health Insurance Portability and Accountability Act of 1996) is a U.S. law that defines privacy and security rules for protecting sensitive patient health information. The law applies to healthcare providers, health plans, healthcare clearinghouses, and any other organizations transmitting health information in electronic form.

HITRUST (Health Information Trust Alliance) is a private company that provides a framework for complying with certain government regulations, including HIPAA. Healthcare organizations often use HITRUST certification to demonstrate their HIPAA compliance.

HIPAA violations can be costly, and breaches – which, by law, must be reported – can be even costlier. Organizations can be fined or required to undertake costly corrective actions, and they might suffer damage to their reputations or even lose customers.

Public cloud providers understand the importance of HIPAA and HITRUST, and they typically offer guidance and resources for constructing HIPAA/HITRUST-compliant environments. Microsoft Azure, for example, offers a Blueprint designed specifically for HIPAA compliance and HITRUST certification.

Establishing a HIPAA-compliant, HITRUST-certified environment on Azure

The Azure Security and Compliance Blueprint for HIPAA/HITRUST – Health Data & AI defines an Azure services architecture for building HIPAA-compliant and HITRUST-certified cloud environments. The Blueprint specifies Azure resources for ingesting, storing, analyzing, and interacting with data as well as for managing identity and security. It includes a sample use case scenario, a deployment template and automation scripts, a security threat model, a list of relevant HIPAA/HITRUST requirements, and more. Designed as a modular foundation, the Blueprint can be adjusted for an organization's specific needs.

The Azure HIPAA/HITRUST Blueprint is an important resource for getting started. It can also serve as a means for evaluating compliance with environments that have already been established. For example, you can use the HIPAA/HITRUST Blueprint to determine whether you have sufficient processes and policies in place to comply with regulations.

Still, the Blueprint does not do everything for you. Ultimately, responsibility for HIPAA and HITRUST compliance rests with your organization.

Whether your organization is considering a move to Azure or you have already built an Azure environment, there are several best practices that can help you achieve HIPAA and HITRUST compliance. These best practices take advantage of the Azure HIPAA/HITRUST Blueprint and draw from Azure services, but in several cases, they might require additional expertise.

Implement key HIPAA/HITRUST best practices

1. Install multi-factor authentication

You need to know exactly who has access to the PHI you have collected. But requiring only a username and password could leave that information exposed to hackers or allow unauthorized use. Multi-factor authentication prompts users for additional information when logging in, asking for a code from a smartphone, or requiring a fingerprint scan, to help ensure the identity of the user.

The Azure HIPAA/HITRUST Blueprint control mappings (which map HIPAA requirements to Azure controls) include recommendations for multi-factor authentication in several situations. For example, the control mappings recommend using multi-factor authentication for all subscription accounts with write privileges to prevent a breach of accounts or resources.

Microsoft offers this enhanced level of security with Azure Active Directory Multi-Factor Authentication, which requires two or more authentication methods:

- Something you know – such as a password
- Something you have – a trusted device that is not easily duplicated, like a phone or hardware key
- Something you are – such as a fingerprint or face scan (biometrics)

There are several versions of Azure Active Directory Multi-Factor Authentication available, each with distinct features and capabilities. Depending on other Microsoft licenses, you may already be entitled to use one of the versions.

2. Configure platform logs

If a breach occurs, you will need an efficient way of determining what happened, when, and who was responsible. A "platform" log, as Microsoft calls it, can provide diagnostic information and an audit trail.

With Azure, there are several types of platform logs:

- Resource logs provide information about operations performed on Azure resources, such as removing a secret from an Azure Key Vault or making a request to a database.
- Activity logs track operations on each Azure resource in a subscription from the outside in addition to updates on Azure Service Health events. These logs can help you determine who is responsible for particular write operations and when those operations occurred. There is one activity log per subscription.
- Active Directory logs include the history of sign-in activity and provide an audit trail of changes made in Azure Active Directory for a particular tenant.

Microsoft provides options for how to view these logs and where to forward them. For example, you might decide to send logs to an analytics workspace. Azure collects all of this information automatically, but only if you configure the logs correctly for a particular destination.

3. Fortify your business continuity strategy

Whether your company is providing healthcare directly to patients or offering services such as data analysis to other organizations, you know that extended downtime is unacceptable. Unexpected outages that last a day or even a few hours could frustrate users, temporarily halt revenue flows, damage your reputation, or potentially threaten the timely delivery of patient care.

Yet those outages can and do happen, even with public cloud environments: floods, fires, power outages, accidents, hardware failures, security breaches, and other events can cause service disruptions.

You might have established a disaster recovery/business continuity strategy for your on-premises data center. But have you updated that strategy now that you have vital apps and data in the cloud? You need a plan that enables you to have all of your resources – from your apps to the databases and stored data they draw from – available again within minutes of an interruption.

The HIPAA Security Rule requires contingency plans. In particular, you must have plans for disaster recovery and emergency operations – and you must have procedures in place for testing and revising those plans.

There is no "one-size-fits-all" strategy for disaster recovery or business continuity when using Azure for healthcare. But your plan will likely include some level of app and data replication across distinct regions in the United States. For example, you might replicate data from an East Coast cloud location to a Central U.S. cloud so that during an East Coast outage, your environment will automatically fail over to the other cloud.

Establishing your plan requires a thorough risk assessment. And – as HIPAA specifies – it requires periodic testing. You need to simulate failovers to make sure they will work as planned during a real event.

4. Back up your data

Your data backup strategy should work hand in hand with your business continuity/disaster recovery plan. In fact, the HIPAA requirement to develop and implement a data backup plan is part of the same Security Rule that contains mandates for business continuity and emergency operations.

Clearly, backing up your data is critical for preventing its loss as a result of an outage, accidental erasure, or some other event. But which data should be backed up? And how frequently should you back it up?

You probably do not need to back up all of your data continuously. For example, you might decide to back up your test and development environment less frequently than components of your patient-facing web application.

To build an effective backup plan along with your disaster recovery and business continuity strategy, you will need to determine:

- Which apps and environments are the most critical for business continuity?
- How much data can you afford to lose in the event of an outage?
- How much time can you afford to be offline while rebuilding environments or failing over to a secondary site?
- What are your commitments or service-level agreements (SLAs) for internal and external users?

And importantly, you need to decide what you are willing to spend to meet all of your technical and business objectives.

5. Strengthen network and storage security – avoid default settings

When you first begin to configure your network and storage environment, you need to make sure you do not inadvertently leave sensitive information exposed to hackers. But by default, Azure storage is open to public internet traffic. Maintaining that default setting could be disastrous for your organization. Hackers could use widely available tools to scan open ports and ultimately gain access to what should be protected data.

Preventing intrusions requires you to restrict access. Although restrictions will vary from one organization to another, you might decide to allow access only from certain IP addresses, public internet IP address ranges, or virtual networks (VNets). Be prepared to fine-tune those restrictions over time. You should regularly review where traffic is coming from and decide whether you need to make adjustments or implement additional restrictions.

As this best practice highlights, the Azure HIPAA/HITRUST Blueprint and default Azure settings will not provide requisite security. The Blueprint can help you assemble all of the necessary resources for setting up your environment, but it is up to you to configure those resources to protect data and achieve HIPAA compliance.

6. Encrypt your data

You need to make sure that if a breach occurs – or if physical hardware is stolen – hackers cannot actually read the data you have stored. At the same time, you need ways to prevent hackers from reading protected data in transit, as it is being transferred from one data center to another or delivered to an authorized person through a web site, mobile app, or email.

Data encryption is an important and effective means of preventing hackers, thieves, and any other unauthorized people from reading sensitive data. When data is encrypted, it requires a confidential process or key to make it readable.

Encryption can be applied to data "at rest," like when it is stored on a hard drive in a data center, as well as "in transit" (or "in flight"), like when it is transferred or delivered to authorized people. HIPAA does not technically mandate encryption as the sole means of securing data as part of its Security Rule, though it requires organizations to use encryption "whenever deemed appropriate."

If your organization exchanges information beyond a single, firewall-protected environment – which you likely do if you are using a public cloud – then encryption is appropriate. Azure offers a variety of at-rest and in-flight data encryption options plus a means to manage keys in a subscription-based Azure Key Vault.

Selecting the right combination of encryption options for your organization could be complicated and will depend on your environment. You might need to actively choose to encrypt data in some areas of your environment, while data in other areas might be encrypted by default. For example, if you are using the Azure Cosmos DB distributed, multi-modal database, then user data is encrypted on its solid-state drives by default. If you are using Azure Blob storage and Azure file shares, you might need to evaluate server- and client-side encryption options.

7. Use robust, role-based access control

To prevent accidental – or intentional, malicious – modification of information and systems, you need to control which users have access to Azure resources, what areas they can access, and what they can do with those resources. For example, you might decide that someone in one particular role should have read-only access to stored information while someone in another role can have write permission.

Azure role-based access control (RBAC) capabilities can help you manage those policies. With Azure RBAC, you define roles, set policies for those roles, establish the scope of resources that someone in a role can access, and more. As you configure access controls, you should consider how many owners you need for each subscription. By default, you might grant the same level of owner access to numerous people. But limiting the number of owners – and assigning other team members to roles such as contributor, reader, or even more specifically something like "virtual machine reader" – can help prevent problems.

The Azure HIPAA/HITRUST Blueprint includes control mappings for this kind of segregation of duties. But implementing that segregation, such as by using Azure RBAC, is your responsibility. Efficiently configuring Azure RBAC could require outside expertise.

8. Sign up for Azure Active Directory Premium

Azure offers paid Active Directory Premium services that augment Azure Active Directory Free. Active Directory Premium is a must-have for undertaking several HIPAA best practices.

Microsoft offers two versions of the premium offering:

- Active Directory Premium P1 supports a range of advanced administration features, including Microsoft Identity Manager access management.
- Active Directory Premium P2 includes all P1 services plus Azure Active Directory Identity Protection (which provides risk-based conditional access), privileged identity management, and access reviews.

The capabilities of Active Directory Premium P2 make it the best choice for healthcare organizations that need to maintain HIPAA compliance with their Azure environment. Privileged identity management, for example, helps you minimize risks by providing time- and approval-based access to particular resources for specific roles. The access reviews available with Premium P2 enable you to regularly review group memberships, access to enterprise applications, and role assignments to make sure only the right people continue to have access.

Though some organizations might be reluctant to pay for a premium Active Directory service, it should be a prerequisite for healthcare organizations using Azure. The added features are essential for preventing breaches that could cost much more than the licenses.

9. Review Azure Security Center frequently

Azure Security Center is an important and very valuable resource for healthcare organizations using Azure. This infrastructure security management system is designed to assist you in managing your security posture and strengthening threat protection for workloads – whether those workloads are running in Azure or on premises. Security Center can help you understand the status of your resources and determine whether they are sufficiently secured. It also analyzes workloads, providing threat prevention recommendations and triggering security alerts when necessary.

Security Center can provide continuous insights. For example, it tracks when you add new resources and determines whether they are configured according to best practices. If there are potential issues, administrators receive recommendations for how to address them.

Still, making the most of Security Center requires continuous attention. An administrator should go into Security Center every day to make sure there are no issues that could cause compliance problems with HIPAA regulations or other rules and standards. Reviewing Security Center daily can help you identify and address any issues quickly before they require more time-consuming and costly remediation efforts.

10. Conduct regular comprehensive reviews

Moving to the cloud is not a single, fixed-term project. Once your environment is up and running on Azure, you need to establish new processes and ongoing management routines.

One of the most important processes should be a regular, comprehensive review of security, operations, and costs. Like a healthcare check-up, you should periodically evaluate how your environment is working and identify any areas where some preventive medicine is in order. Ask yourself:

- Are there any security gaps that should be addressed?
- Are any services underutilized – and could you move to more cost-effective services?
- Do you need to scale up performance or capacity for particular workloads?

Part of that periodic check-up should include an analysis of how any new technologies you are employing comply with HIPAA rules. For example, if you launch a new app that taps into Azure AI or machine learning (ML) capabilities, you should evaluate whether you need to make any changes to security or access management to sustain compliance.

Maintain HIPAA compliance and HITRUST certification with Cloudticity Oxygen

The Cloudticity Oxygen™ managed cloud solution can help your organization properly configure your environment for HIPAA compliance and HITRUST certification – and it can help you maintain compliance and certification going forward. Oxygen is the world's first and only 99 percent autonomous managed cloud solution for the healthcare industry. It automates the delivery of managed services, managed security, and managed compliance for Azure, implementing thousands of continuous compliance checks. Capitalizing on ML, Oxygen identifies and automatically remediates any drifts in your compliance posture.

Beyond providing the innovative Oxygen managed cloud solution, Cloudticity offers deep expertise in empowering healthcare organizations to launch and maintain cloud-based healthcare solutions. Since our founding in 2011, we have helped organizations deliver some of the healthcare industry's first solutions in the cloud.

Cloudticity firsts for healthcare in the cloud include:

- First patient portal in the cloud
- First health information exchange in the cloud
- First Meaningful Use Stage 2 (MU2) compliance attestation for a large hospital system

As an Azure Silver Partner, we also have the knowledge and experience to help you select and configure the Azure solutions you need for HIPAA compliance. We help you build on the Azure HIPAA/HITRUST Blueprint, providing substantially more control mappings to address precise HIPAA requirements with the right policies and solutions. We help you build solutions that are not only compliant and secure but also make the most efficient use of Azure services to support your business goals.

To implement best practices, we can help you:

- Select Azure services for multi-factor authentication and encryption
- Configure platform logs
- Properly restrict network and storage access
- Establish and test business continuity plans
- Design and implement backup strategies
- Set up access control parameters
- Deploy Azure Active Directory Premium P2

Importantly, we deliver continuous, ongoing managed services.

- **Managed services:** We provide Well-Architected public cloud infrastructure backed by 24×7×365 helpdesk coverage with incident escalation for urgent issues. We also provide automated backups, logging, and complex automated patching scenarios as well as automated regional disaster recovery.
- **Managed security:** We provide a virtual Security Operations Center (vSOC) backed by HITRUST-certified Cloudticity Oxygen, with capabilities for intrusion detection and prevention, log monitoring, file integrity monitoring, and real-time malware prevention. We review Azure Security Center daily to identify any emerging security or compliance issues.
- **Managed compliance:** Oxygen performs over 1,000 continuous compliance checks that scan environments according to HIPAA and HITRUST definitions. It automatically remediates 99 percent of compliance deviations. For any deviations that are not addressed automatically, Oxygen generates alerts through a real-time compliance dashboard and presents recommended remediation options.
- **Continuous optimization:** We also provide regular, comprehensive reviews of security, operations, and costs so you can optimize your environment. In addition, we will help you evaluate and capitalize on emerging technologies while assessing the impact of those technologies on HIPAA and other standards and regulations.

Get Started

Ensuring HIPAA compliance and achieving HITRUST certification for a cloud environment can seem daunting. With Cloudticity Oxygen, you can meet compliance and certification requirements while freeing your team to focus on product development and innovation. With Cloudticity, offloading administrative tasks is as simple as using a software-as-a-service (SaaS) platform.

For more information about how Cloudticity can help your organization achieve and maintain HIPAA compliance and HITRUST certification on Azure, speak with one of our Azure healthcare specialists today.


cloudticity
Get Ready With Automated Managed Services Today
SPEAK WITH A SPECIALIST