cloudticity

Achieve HIPAA Compliance on AWS - 11 Best Practices

Table of Contents

The Need for HIPAA Compliance

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 electronic protected health information (ePHI), 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.

This Ebook looks at 11 best practices organizations should follow when running healthcare workloads in Amazon Web Services (AWS).

The AWS Shared Security Model

The first step to properly securing AWS is understanding the shared responsibility model. AWS and the customer share the responsibility for security and compliance in the cloud. AWS is responsible for the security of the cloud. This overall consists of the security of the hardware, software, networking, and physical facilities that comprise the cloud infrastructure.

The customer is responsible for the security in the cloud, which pertains to the data and resources they deploy in the cloud. These responsibilities include:

- Securing electronic protected health information
- Implementing identity and access management (IAM) for platforms and applications
- Configuring operating systems, networks, and firewalls
- Encrypting client-side and server-side data
- Protecting network traffic with encryption and performing identity authentication

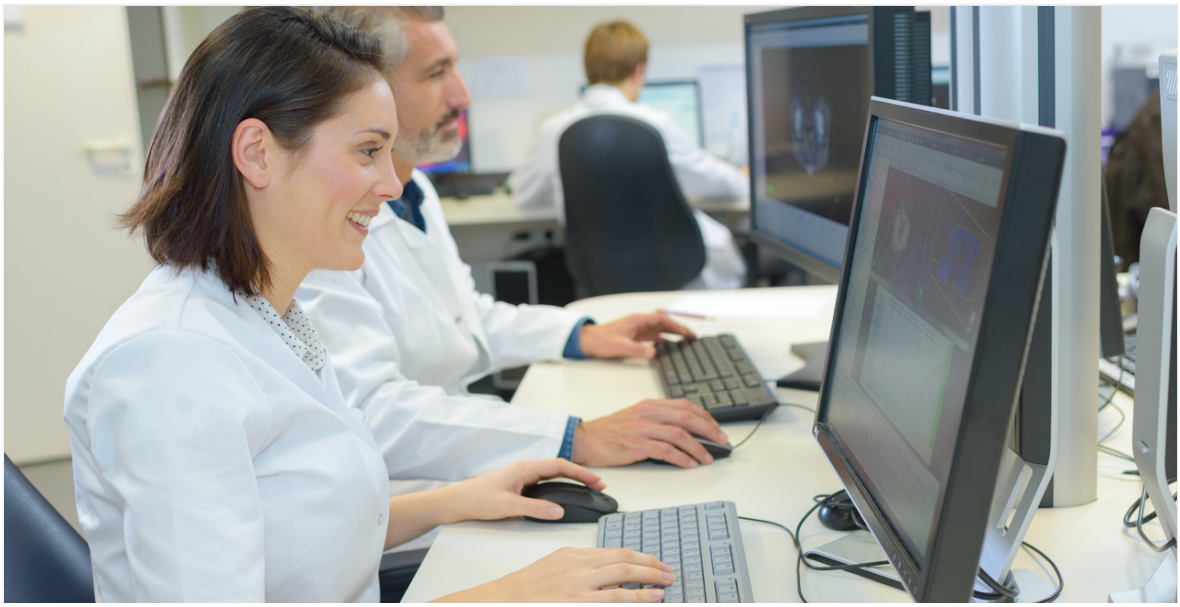
It is important that customers fully understand the shared responsibility model and its implications when constructing an HIPAA-compliant environment. AWS provides a secure infrastructure that healthcare companies can use as the foundation of a computing landscape that complies with HIPAA standards, but it is ultimately up to the customer to ensure the security of the data they store and process in the cloud.

Best Practices To Ensure HIPAA Compliance in AWS

The following best practices will help healthcare companies remain compliant with HIPAA standards. They all address aspects of security designated as part of the customers' responsibilities in the shared security model.

1: Inventory your systems and tag ePHI

It is impossible to protect ePHI resources if you don't know which systems they reside in and which applications interact with them. The first best practice a company should engage in is to perform a complete inventory of the cloud services, infrastructure components, and containers that are used to store, process, or transmit ePHI. Once you identify and tag the relevant resources, you can assess risks and address any gaps. Tagging your resources properly will help you simplify compliance management going forward, allowing you to easily filter for ePHI resources and manage the security settings for those particular components.



2: Encrypt ePHI at rest and in transit

The overriding motivation behind HIPAA is to protect patient health information and restrict any possibility of unauthorized access. When dealing with ePHI, fulfilling this requirement demands that you encrypt all ePHI throughout its lifecycle. This means you should encrypt ePHI both at rest and in transit.

You can implement encryption in your AWS environment using a variety of methods. Commercial and open-source encryption tools are readily available. Customers can take advantage of Amazon's Elastic Block Store (EBS) which provides transparent encryption of data residing on its volumes. Encryption keys need to be protected, and it is good practice to rotate the keys at least every 90 days.

Customers need to ensure that ePHI is encrypted in transit with methods such as combining Transport Layer Security 1.2 (TLS) with an industry-standard AES-256 cipher. AWS recommends that encryption in transit should be set up for all clients accessing regulated data resources. Environments using the Amazon Elastic File System (EFS) can configure IAM policies to enforce encryption in transit.

Protecting ePHI includes backing it up regularly to protect against accidental deletion or other forms of human error. Backups are an essential component of a disaster recovery plan, which we will discuss in more detail shortly. Backups should also be encrypted and the backup media protected against loss or theft.

3: Configure your firewalls

You should configure all hardware, software, and web application firewalls to keep unauthorized users out of your systems. The goal is to restrict the flow of network traffic on networks with access to ePHI. Multiple firewalls can be involved in a complex environment, and each one poses a potential risk to sensitive data resources.

You should adhere to the following five basic configuration best practices when configuring the firewalls in a HIPAA-compliant infrastructure.

Segment networks employed by different parts of the business with security setting customized for each segment.

- Update firewall rules to address issues such as default accounts and passwords or outdated software.
- Virtual private networks (VPNs) should be used for all remote access to ePHI systems.
- Inbound and outbound rules need to be configured to control what comes into or goes out of your network.

Network segmentation protects the environment from vulnerabilities that may affect one part of the business. For example, having email systems on a different network segment or separate AWS account from the apps processing electronic health records (EHRs) provides additional protection to ePHI resources. A successful phishing expedition aimed at the email system will not be able to compromise the systems containing regulatd datae.

4: Restrict and monitor access to ePHI resources

Both external actors or internal users can perpetrate data breaches. You can mitigate the risks by restricting access to the data through the use of role-based policies. Providing access to ePHI systems should **never be the default** when provisioning new user credentials or configuring IAM policies. As a best practice, access controls should follow the least privilege rule, meaning you should grant the minimum number of access privileges needed for each person to do their job.

Technical safeguards defined in the HIPAA Security Rule specify four aspects that need to be incorporated into a covered entity's access controls:

- Every user must have a unique ID or identifier that allows their activity to be tracked when working with ePHI.
- Emergency access procedures must be in place that inform users how to obtain ePHI in urgent situations. Access controls may need to be modified in the event of an emergency procedure.
- Automatic logoff should be implemented where possible to limit unauthorized access to ePHI.
- Encryption and decryption need to be implemented on all data transmissions involving ePHI.

Monitoring and auditing user activity in your AWS environment is also the customer's responsibility. To help you do this, AWS Cloudtrail logs should always be enabled. This will allow you to investigate anomalous behavior and ensure your resources are being managed in a compliant way.

5: Implement multi-factor authentication (MFA) on IAM identities

The expanding remote workforce increases the importance of enforcing multi-factor authentication (MFA). Individuals may be accessing regulated systems from mobile devices or workstations in home offices. Therefore, companies must implement IAM policies that prevent unauthorized access, like MFA.

Companies should enforce MFA for all users accessing systems that contain or process ePHI. AWS provides the facility to implement MFA on a per-user basis, but it is the customer's responsibility to activate this functionality.

6: Minimize your attack surface area

Hackers are notoriously tenacious and are continuously looking for ways to compromise your systems and gain access to your valuable data. A tested method of hacking into systems and networks is through the use of default credentials to access a company's applications or devices. Fortunately, you can address this vulnerability easily.

You should change all default admin credentials accompanying software or hardware components in a prospective HIPAA-compliant AWS environment when you introduce them into the infrastructure. You should also change passwords regularly and whenever individuals leave or join a team.

Another way to reduce the attack surface in an AWS cloud environment is to minimize your operating system (OS) exposure. You can do this by removing all OS components that are not needed to perform a system's designated tasks. Unnecessary and unused software just leaves more doors open to possible misuse by malicious actors and should be avoided to better protect your ePHI. If a software component is not required to get the job done, you should remove it from the system.

7: Update antivirus products and security patches regularly

The threat of virus or malware infection is constantly evolving as hackers devise new techniques to comprise your systems. Malware is dangerous in any computing environment but can be devastating when it leads to a data breach.

Healthcare organizations need to be proactive in addressing the danger of malware by maintaining effective antivirus software throughout the AWS environment. You should set the antivirus programs to automatically install new updates as they become available. The corporate policy should insist on antivirus software being installed on any user's mobile device that will access systems containing ePHI.

In addition to keeping antivirus software updated with the newest threat databases, all systems should have new security patches installed as soon as possible. Developers regularly find and address vulnerabilities in their products through these patches, and it is the customer's responsibility to install them in the environment. Some anti-malware systems provide interim protection via virtual patching until official patches can be tested and applied.

8: Implement a robust contingency plan

A contingency plan, also called a disaster recovery plan or business continuity strategy, is an essential component of the HIPAA administrative safeguards. The HIPAA Contingency Plan standard requires organizations to anticipate how ePHI systems could be damaged by natural or man-made disasters. Companies need to create procedures and policies that address these situations to remain HIPAA-compliant.

The National Institute of Standards and Technology (NIST) suggests developing a contingency plan using the following seven steps.

1. Develop a formal contingency planning policy statement that provides the necessary corporate authority and guidance to enact the plan.

2. Conduct a business impact analysis (BIA) to inventory and identify critical systems that need priority handling. In a healthcare organization, these systems would include those directly related to the storage and processing of ePHI.

3. Identify measures that can be implemented to reduce the effects of system outages and enhance availability, thereby limiting the costs involved with enacting contingency activities.

4. Recovery procedures and strategies need to be developed for every system that will be recovered in the event of a disaster. The procedures have to include backing up the systems at an acceptable frequency. Procedures should be reviewed and updated regularly to reflect changes in the environment.

5. An all-encompassing IT contingency plan is required to provide timetables, prerequisites, and procedures for restoring systems in an emergency.

6. Testing an organization's contingency plan is a critical activity that helps to identify gaps in planning and enables teams to practice their preparedness for a real event. Tests should be planned regularly with extensive reviews to discuss their outcome and suggest potential plan refinements.

7. The contingency plan is a living document that must reflect the current environment. It needs to be updated regularly, such as whenever new systems are added or deleted from the IT inventory.

9: Conduct periodic risk assessments and analyses

The first best practice we discussed was inventorying systems for ePHI. Additionally, organizations are responsible for performing periodic risk assessments and analyses. This assessment is designed to identify any vulnerabilities that might affect the integrity, confidentiality, or availability of ePHI. The organization must then address any vulnerabilities discovered during the process.

The risk assessment consists of four main parts designed to keep ePHI secure.

- Systems that store, transmit, or process ePHI need to be identified.
- All vulnerabilities that may put ePHI at risk should be identified and documented.
- Threats and current security measures need to be assessed and documented.
- Risk levels need to be assigned to all of the identified vulnerabilities.

At the conclusion of the risk assessment, organizations should have a risk management process in place to quickly address findings that can lead to HIPAA violations. Known vulnerabilities that are not resolved promptly can result in excessive penalties for willfully ignoring HIPAA regulations.

Failure to perform and document risk analysis and address vulnerabilities is a very common HIPAA violation that can lead to large financial penalties. Fines have been levied against major healthcare providers as well as individual doctors.

10: Perform regular employee training

All workforce members of HIPAA-designated covered entities (CEs) and business associates (BAs) need to be trained on HIPAA Privacy and Security Rules. This refers to all employees, contractors, and consultants working for the CE/BA regardless of their level of interaction with ePHI.

All new members of the workforce need to be trained as part of the onboarding process. Training should also be immediately initiated when new systems or procedures related to the processing of ePHI are introduced into the environment.

HIPAA guidelines are somewhat nebulous and require periodic and ongoing training. Most companies perform this training yearly as a best practice and retain documentation verifying that all individuals completed the training materials for audit purposes.

11: Work with a reputable managed services provider (MSP)

In many cases, the complexities of maintaining a HIPAA-compliant environment taxes the capabilities of in-house IT teams. HIPAA is a constantly evolving regulation, and different healthcare organizations have different requirements of their vendors.

There is also a cloud computing skills shortage affecting all industries. Training staff is a costly proposition for healthcare organizations, and even if your staff can learn new skills they still lack valuable experience.

That's why 70% of companies are partnering with a managed services provider (MSP) for IT operations. The right MSP will not only help you augment the skills shortage and mitigate cybersecurity threats – it will also enable you to focus internal resources on more strategic activities that drive your business forward.

Consider Cloudticity Your MSP

When choosing a cloud partner for a healthcare organization, it's important to consider several critical things:

1. **Healthcare experience:** Many cloud partners claim to have numerous years healthcare experience, but many of them are generalists. Work with a partner that not only has extensive cloud experience, but specializes in healthcare and the relevant compliance frameworks such as HIPAA, HITRUST, FISMA, and NIST.

2. **HITRUST status:** It should go without saying that your MSP partner should be HITRUST certified. But also look at HITRUST status. Some partners are part of the HITRUST Inheritance Program which can offer you significant benefits when it comes to helping you obtain certification.

3. **Cloud credentials:** AWS provides a catalog of healthcare and government-related certifications that its partners can work to obtain, such as the Healthcare Competency and Public Sector Partner Competency, as well as validated technology competencies, such as the Audited Managed Service Provider credential and DevOps Competency certification.

4. **Co-management:** Many MSPs will require full control over your production environment to enable management. This means that you have to go through their service desk to make any change, however large or small. Look for an MSP that provides a co-management model. Cloudticity allows you to own your production environment, we just deploy our managed cloud solution which enables the monitoring.

5. **Partnership:** An MSP should feel like an extension of your internal team. Look for a partner that with SLAs in place that ensure they won't leave you scrambling in the event of an outage. Cloudticity provides a 15-minute SLA for urgent production issues 24/7/365.

Cloudticity meets all these requirements and has been helping healthcare organizations be successful on the public cloud for over ten years. We've built some of the earliest and largest systems on the public cloud, including:

- The first patient portal
- The first Health Information Exchange
- The first Meaningful Use 2 Compliance attestation for a large hospital system
- The first COVID-19 registry for a state health department

We'd love to help you on your cloud journey.
Schedule a free consultation to learn more today.

Assess Your Current State of HIPAA Compliance

It's a good idea to conduct a risk assessment of your AWS environment to uncover any compliance gaps. Take advantage of Cloudticity's free AWS Technical Assessment. The automated tool scans your AWS environment and reports on how your account compares to industry standards for compliance as well as security, reliability, and cost optimization.


cloudticity
Is Your AWS Account Ready for Healthcare? Get Your Free AWS HIPAA Assessment Today
GET STARTED NOW