Clearwater

Top HIPAA Risks and Misconfigurations

in AWS Environments

Not every cloud platform is the same. When it comes to HIPAA, there are unique risks and misconfigurations within Amazon Web Services (AWS) environments that we will look at from the data of Office for Civil Rights (OCR) enforcement findings, industry trends, and audits.
Details from OCR enforcement actions related to AWS environments were similar to those found in Azure environments. While the details are different due to the variety of options and services between the two, the focus was on incorporating cloud-based assets into HIPAA Risk Analysis, and common data protection errors of weak access management, lack of logging and missing encryption.

Here in this list are the top AWS cloud risks and misconfigurations that any healthcare organization should be prioritizing. Take a closer look at the services that Clearwater can provide in security and cloud posture management for AWS and other cloud platforms to avoid these issues or contact us for more information.

OCR HIPAA Cloud Risk Overview

Improper Risk Analysis That Excludes AWS Resources as Assets

OCR repeatedly penalizes organizations that fail to include AWS-hosted cloud-based assets in their HIPAA risk analysis.

- Many covered entities don't document or assess the risks to EC2 instances, S3 buckets, RDS databases, or cloud-based backups.
- OCR expects cloud-hosted ePHI to be treated with the same rigor as on-prem assets under 45 C.F.R. §164.308(a)(1)(ii)(A).

OCR HIPAA Cloud Risk Overview (cont'd)

S3 Bucket Misconfigurations (Exposed ePHI)

One of the most frequent and dangerous risks: publicly accessible S3 buckets that expose sensitive files.

Common missteps:
- Leaving S3 permissions open to "Everyone"
- Failing to enable object-level logging or versioning
- Lack of server-side encryption (SSE-S3 or SSE-KMS)

This risk has led to multiple large-scale healthcare breaches, including open ePHI backups and files indexed by search engines.

Insufficient Identity & Access Management (IAM) Controls

Weak IAM policies in AWS can result in unauthorized access to ePHI.

Common issues:
- Overly permissive IAM roles
- Failure to enforce least privilege
- Lack of MFA on IAM users or root accounts
- Misuse of temporary credentials or hardcoded access keys

OCR emphasizes strong IAM as a technical safeguard under 45 C.F.R. §164.312(a).

Lack of Logging & Monitoring (Audit Controls)

HIPAA requires audit logging to track access to ePHI, per 45 C.F.R. §164.312(b).

Many organizations fail to:
- Enable AWS CloudTrail or don't store logs in a tamper-evident location
- Monitor unauthorized API calls or privilege escalations
- Set up CloudWatch alerts for anomalous behavior

OCR views insufficient logging as a sign of poor visibility and weak incident detection capability.

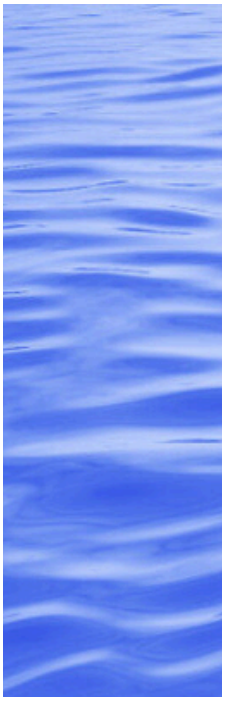
OCR HIPAA Cloud Risk Overview (cont'd)

Unencrypted Data at Rest or in Transit and in Backups

AWS offers multiple encryption options; however, OCR audits have pointed out their lack of use. Organizations were cited for:

- Failing to enable S3 default encryption
- Did not configure or use TLS for inter-service communications
- Storing snapshots, RDS backups, or EBS volumes unencrypted
- Not encrypting backup data if AWS is the offsite source
- Lack of monitoring backup access
- Lack multi-region redundancy for availability (required under 45 C.F.R. §164.306)

OCR treats unencrypted ePHI as a high-risk violation unless a strong justification is documented under the "addressable" safeguard provision.



Why Clearwater for Cloud Security & Compliance Assistance?

As the largest purely healthcare-focused provider of managed security and compliance programs, we possess deep expertise and extensive experience working with healthcare organizations and businesses. We can tailor a program that meets your security, compliance, and resiliency needs, designed to scale with your business.

Some of our related services to consider with AWS environments for healthcare businesses:

- Cloud Security & Compliance Assessments, determine the gaps in security and compliance management across your environment (HIPAA, NIST 800-171, and more).
- Cloud Cyber Risk Management, 24/7 monitoring and assistance to quickly identify the risks outlined here and others, leveraging an industry-leading cloud security posture management platform managed by healthcare cloud experts.

Clearwater helps organizations across the healthcare ecosystem move to a more secure, compliant, and resilient state so they can achieve their missions. The company provides a deep pool of experts across a broad range of cybersecurity, privacy, and compliance domains, purpose-built software that enables efficient identification and management of cybersecurity and compliance risks, managed cloud services, and a 24/7 Security Operations Center with managed threat detection and response capabilities.