Clearwater

Top HIPAA Risks and Misconfigurations

in Microsoft Azure Environments

Not every cloud platform is the same. Regarding HIPAA, there are unique risks and misconfigurations within Azure Cloud environments that Clearwater has identified from recent Office for Civil Rights (OCR) enforcement actions, as well as what our consultants have seen from Azure Cloud Security Assessments.

OCR enforcement findings focus on the broad areas where cloud assets were not fully accounted for in an organization's HIPAA risk analysis, which led to HIPAA violations. From our consultants, the findings were more aligned with a deficiency in maturity needed to manage access and identity management spanning Microsoft applications and services, and across Azure Cloud tenants to keep patient data safe.

Two views of HIPAA risks combined to deliver one list of Microsoft and Azure cloud risks and misconfigurations that any healthcare organization should be prioritizing.

OCR HIPAA Cloud Risk Overview

Incomplete or Inaccurate Risk Analysis (Not including Azure services in the assessment)

OCR's #1 cited violation. Many healthcare entities fail to fully account for Azure-hosted assets in their HIPAA risk analysis.

Omitting Azure virtual machines, SQL databases, Blob storage, and backups from formal assessments led to an incomplete or inaccurate Risk Analysis.

OCR enforcement actions in 2024 and 2025 explicitly penalized healthcare entities for risk analysis deficiencies tied to Azure environments and systems. OCR flagging the same deficiency: **inadequate cloud-aware risk analysis**.

Misconfigured Azure Blob Storage or File Shares

Just like AWS S3, Azure Blob storage misconfigurations frequently lead to public exposure of ePHI. Common issues:

- Anonymous read access enabled
- No encryption at rest or in transit
- Public URL access to PHI files or logs
- Shared Access Signatures (SAS tokens) with no expiry

OCR treats unprotected storage containers as a violation of both the Security Rule and Privacy Rule if patient data is exposed.

Overly Permissive Azure Role-Based Access Control (RBAC)

Improper implementation of Azure Active Directory (AAD) roles is a widespread weakness. Risky practices:

- Global Administrator assigned to everyday users
- Broad access across subscriptions or tenants
- Lack of MFA for privileged accounts

OCR expects least privilege access and role-based controls for all systems interacting with ePHI under 45 C.F.R. §164.312(a).

Disabled or Incomplete Audit Logging

OCR enforcement consistently cites failure to maintain and review audit trails, a key safeguard under 45 C.F.R. §164.312(b).

Azure-specific gaps:

- Microsoft Defender for Cloud not enabled
- Activity logs not exported or retained
- No alerting on suspicious behavior in AAD or Sentinel

Failing to detect or investigate unauthorized access increases exposure time—and OCR penalties.

Unencrypted Data in Azure Storage or Databases

Encryption is “addressable” under HIPAA but strongly expected by OCR—especially in the cloud.

Common gaps:

- Azure SQL Database encryption not enabled
- Blob storage without Microsoft-managed or customer-managed keys
- Unprotected backups or unmanaged VM disks

OCR often cites lack of encryption as a failure to “reasonably and appropriately safeguard” ePHI.

Assuming Azure’s Business Associate Agreement Covers All Services

Microsoft’s BAA only includes **specific Azure services** designated as HIPAA-eligible.

- Using **unsupported services** (e.g., Power BI, Logic Apps, Azure OpenAI, Azure DevTest Labs) may place ePHI at risk and **outside compliance scope**.
- Many organizations assume the full Microsoft Cloud is HIPAA-covered—it isn’t.

OCR holds covered entities liable if ePHI is processed using non-covered services—even if Microsoft signed a BAA.

Missing or Weak Backup and Disaster Recovery in Azure

OCR enforcement includes failures under 45 C.F.R. §164.308(a)(7) (Contingency Plan).

Common issues:

- No replication across regions
- No test of restore procedures
- Incomplete backup of ePHI in Azure Backup, Azure Site Recovery, or third-party integrations

Azure HIPAA Risks Identified from Clearwater Security Assessments Overview

Insecure User Consent Settings

Malicious actors often utilize Entra ID-registered applications to conduct phishing attacks against organizations. With misconfigured user consent settings, any user within the tenant could consent to access to malicious Entra ID applications hosted in a foreign Azure tenant.

Insecure User Consent Settings (cont'd)

This results in an Illicit Consent Grant Attack. A malicious actor might be able to trick users into granting permissions to modify and access data within the Azure environment.

Misconfigured user consent settings might allow malicious actors to phish users and access sensitive patient data within OneDrive and SharePoint. Additionally, this might allow malicious actors to compromise client workstations by modifying files and deploying malware within OneDrive.

Preventative Measures

- Only allow users to consent to verified publishers' apps
- Implement Admin Consent Workflow for unverified publishers' apps and disable User Consent to any applications.

Insecure Entra ID Group Permissions

Entra ID groups can be assigned various roles and access rights, which are applied to all members of the group. A group with misconfigured permissions might allow malicious actors to modify group permissions and memberships. As a result, a malicious actor might be able to modify the insecure groups to inherit additional roles and permissions.

Depending on the roles attached to the misconfigured group, a malicious actor might be able to access privileged Azure resources, including storage accounts, virtual machines, and other services. It is also worth noting that these groups could have privileged roles that might allow malicious actors to enact password changes and elevate privileges. With elevated access to Azure, malicious actors could deny access and modify sensitive patient data.

Preventative Measures

- Review group permissions and membership rules associated with the Azure AD tenant
- Delegate group editing permissions to required personnel

Weak Password Policies

Weak password policies enable malicious actors to easily compromise accounts and breach an organization's Azure tenant. Weak passwords consist of frequently guessable passwords or combinations, such as the current season followed by the current year. Weak passwords undermine the security of the entire Azure tenant, since malicious actors often conduct password spraying attacks against the tenant's users.

As a result of a weak password policy, malicious actors could compromise tenant accounts, enabling them to access sensitive resources. These resources might consist of sensitive patient documents stored in storage accounts or in Microsoft 365 related services, such as SharePoint and OneDrive. Additionally, it is worth noting that malicious actors could also exploit the permissions of the compromised user to elevate privileges within the tenant, this might allow the attacker to compromise the entire Azure estate.

Preventative Measures

- Enforce multi-factor authentication (MFA) for all healthcare system accounts.
- Have robust password requirements, combining alphanumeric, symbols, and varied case characters.

By giving greater attention to their Azure Cloud environment during their HIPAA Risk Analysis and taking the preventative steps outlined above, healthcare organizations can avoid many of the security issues that commonly arise.

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:

- Managed Security for Azure Cloud, M365, including hybrid cloud configurations. Protecting healthcare ePHI and innovation for digital health companies.
- Planning and Migration services enabling HIPAA-compliant environments within Microsoft Azure.
- 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 with 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.