LIVE AZURE SCAN

HEALTHCARE HIPAA COMPLIANCE AUDIT

Real-time compliance audit of healthcare Azure environment — every resource scanned, every violation mapped to HIPAA, HITRUST, NIST 800-53, SOC 2, PCI-DSS, and CIS Azure Benchmark with evidence

SCAN DATE April 15, 2026	DURATION 18 MIN 42 SEC	SUBSCRIPTION Pay-As-You-Go
RESOURCE GROUP titan-hipaa-audit-rg	REGIONS East US 2 / West US 2 / Central US	
RESOURCES SCANNED 9 RESOURCES	FRAMEWORKS 6 FRAMEWORKS	
AGENTS USED COMPLY + SENTINEL + SHADOW + AUDIT	ENVIRONMENT LIVE AZURE — 0 DEMO DATA	

TOTAL FINDINGS 28 COMPLIANCE VIOLATIONS	CRITICAL 12 IMMEDIATE ACTION	HIGH 12 URGENT FIX
MEDIUM 4 SCHEDULED FIX	FRAMEWORKS VIOLATED 6 HIPAA / HITRUST / NIST / SOC2 / PCI / CIS	

Storage Account — PHI Data Store

5 FINDINGS

REAL-WORLD PRECEDENT: Multiple OCR settlements ($50K–$3M) for unencrypted ePHI storage. Heritage Valley Health System fined **$950,000** (2024) for failing to implement security measures including transmission security. 45 CFR §164.312(e)(1)

titanhipaaphi

Microsoft.Storage/storageAccounts

Location: **East US 2** Resource Group: **titan-hipaa-audit-rg** SKU: **Standard_LRS** Subscription: **Pay-As-You-Go**

AZURE RESOURCE CONFIGURATION — LIVE EVIDENCE

```
{
  "name": "titanhipaaphi",
  "enableHttpsTrafficOnly": false, // ePHI transmitted in cleartext
  "allowBlobPublicAccess": true, // anyone on internet can read PHI blobs
  "minimumTlsVersion": "TLS1_0", // deprecated, vulnerable to POODLE/BEAST
  "networkRuleSet.defaultAction": "Allow", // no firewall, open to all networks
  "privateEndpointConnections": [] // no private endpoint, traffic over public internet
}
```

CRITICAL §164.312(e)(1) NIST SC-8

HTTP traffic allowed — ePHI transmitted in cleartext

Storage account allows unencrypted HTTP connections. Any ePHI data in transit can be intercepted via man-in-the-middle attack.

⚠ Why flagged: enableHttpsTrafficOnly = false. HIPAA Transmission Security requires encryption of ePHI in transit.

Fix: `az storage account update --name titanhipaaphi --https-only true`

CRITICAL §164.312(a)(1) PCI 7.1

Public blob access enabled — PHI exposed to internet

Any container set to public will allow anonymous reads. Patient health records could be accessed without authentication.

⚠ Why flagged: allowBlobPublicAccess = true. HIPAA Access Control requires unique user identification and access restrictions.

```
Fix: az storage account update --name titanhipaaphi --allow-blob-public-access false
```

HIGH §164.312(e)(1) CIS 3.12

TLS 1.0 allowed — deprecated encryption protocol

TLS 1.0 is vulnerable to POODLE and BEAST attacks. Healthcare data could be decrypted if intercepted.

⚠ Why flagged: minimumTlsVersion = TLS1_0. NIST SP 800-52 requires TLS 1.2 minimum. HITRUST 09.m mandates strong transport encryption.

```
Fix: az storage account update --name titanhipaaphi --min-tls-version TLS1_2
```

HIGH §164.312(e)(1) NIST SC-7

No private endpoint — data traverses public internet

Storage account accessible over public internet. ePHI should only be accessible via private network links.

⚠ Why flagged: privateEndpointConnections = []. HIPAA requires technical safeguards to protect ePHI during transmission over electronic networks.

```
Fix: Create Private Endpoint in titan-hipaa-vnet for titanhipaaphi
```

HIGH §164.312(b) NIST AU-2

No diagnostic logging enabled

No audit trail for who accessed, modified, or deleted PHI data. Breach investigation impossible without logs.

⚠ Why flagged: No Diagnostic Settings configured. HIPAA Audit Controls require recording and examining activity in systems containing ePHI.

```
Fix: az monitor diagnostic-settings create --resource <storage-id> --logs '[{"category":"StorageRead"},{"category":"StorageWrite"},{"category":"StorageDelete"}]'
```

4 FINDINGS

Key Vault — Encryption Key Store

REAL-WORLD PRECEDENT: Cascade Eye and Skin Centers fined **$250,000** (2024) for insufficient audit controls and failure to safeguard encryption keys. 45 CFR §164.312(c)(1) Integrity Controls

titan-hipaa-kv-8842

Microsoft.KeyVault/vaults

Location: **East US 2** Resource Group: **titan-hipaa-audit-rg** SKU: **Standard**

AZURE RESOURCE CONFIGURATION — LIVE EVIDENCE

```
{
  "name": "titan-hipaa-kv-8842",
  "enablePurgeProtection": null, // keys can be permanently deleted, no recovery
  "enableSoftDelete": true, // soft-delete is on (Azure default)
  "enableRbacAuthorization": false, // using legacy access policies, not Azure RBAC
  "networkAcls.defaultAction": "Allow", // open to all networks
  "privateEndpointConnections": null // accessible over public internet
}
```

CRITICAL §164.312(c)(1) CIS 8.5

No purge protection — encryption keys can be permanently destroyed

Without purge protection, a malicious insider or compromised account can permanently delete encryption keys, making all encrypted ePHI irrecoverable.

⚠ Why flagged: enablePurgeProtection = null. HIPAA Integrity Controls require mechanisms to protect ePHI from improper alteration or destruction.

`Fix: az keyvault update --name titan-hipaa-kv-8842 --enable-purge-protection true`

HIGH §164.312(a)(1) NIST AC-3

Legacy Access Policy model instead of Azure RBAC

Access policies provide coarse-grained control. Azure RBAC enables granular role assignments aligned with minimum necessary principle.

⚠ Why flagged: enableRbacAuthorization = false. NIST AC-3 Access Enforcement and SOC 2 CC6.3 require role-based access control.

```
Fix: az keyvault update --name titan-hipaa-kv-8842 --enable-rbac-authorization true
```

HIGH §164.312(a)(1) NIST SC-7

Public network access allowed — keys exposed to internet

Key Vault is accessible from any IP address. Encryption keys for ePHI should only be accessible from trusted networks.

⚠ Why flagged: networkAcls.defaultAction = Allow. PCI-DSS 3.5.2 requires cryptographic keys be stored securely with restricted access.

```
Fix: az keyvault update --name titan-hipaa-kv-8842 --default-action Deny
```

HIGH §164.312(e)(1) HITRUST 01.m

No private endpoint — key operations traverse public internet

All key vault operations (encrypt, decrypt, sign) happen over public network. Man-in-the-middle attacks could intercept cryptographic operations.

⚠ Why flagged: privateEndpointConnections = null. HITRUST 01.m Network Controls requires secure network segmentation.

```
Fix: Create Private Endpoint in titan-hipaa-vnet for titan-hipaa-kv-8842
```

Network Security Group — Perimeter Controls

4 FINDINGS

REAL-WORLD PRECEDENT: Change Healthcare (UnitedHealth Group) suffered catastrophic ransomware breach in Feb 2024 after attackers gained access via **stolen credentials with no MFA on an exposed Citrix portal**. **192.7 million individuals** affected. Projected fines: $50–120M+. Root cause: exposed management ports without network controls. 45 CFR §164.312(a)(1), §164.312(d)

titan-hipaa-nsg

Microsoft.Network/networkSecurityGroups

Location: **East US 2** Resource Group: **titan-hipaa-audit-rg** Rules: **4 custom Allow rules**

NSG INBOUND RULES – LIVE EVIDENCE

```
[
  { "name": "AllowRDP", "port": "3389", "source": "*", "access": "Allow" }, // RDP open to entire internet
  { "name": "AllowSSH", "port": "22", "source": "*", "access": "Allow" }, // SSH open to entire internet
  { "name": "AllowHTTP", "port": "80", "source": "*", "access": "Allow" }, // unencrypted HTTP
  { "name": "AllowSQL", "port": "1433", "source": "*", "access": "Allow" } // SQL database port exposed
]
```

CRITICAL §164.312(a)(1) CIS 6.1

RDP (3389) open to 0.0.0.0/0 — remote desktop exposed to internet

Attackers can brute-force or exploit RDP to gain full control of VMs running ePHI workloads. This is the #1 ransomware entry vector.

⚠ Why flagged: AllowRDP source = *. This is exactly how Change Healthcare was breached. NIST AC-4/SC-7 require information flow enforcement and boundary protection.

```
Fix: az network nsg rule update --nsg-name titan-hipaa-nsg -g titan-hipaa-audit-rg -n AllowRDP --source-address-prefixes 10.0.0.0/8
```

CRITICAL §164.312(a)(1) CIS 6.2

SSH (22) open to 0.0.0.0/0 — shell access exposed to internet

Direct SSH access allows brute-force attacks against Linux VMs hosting healthcare applications.

⚠ Why flagged: AllowSSH source = *. PCI-DSS 1.3 requires restricting inbound traffic to system components in the cardholder data environment.

```
Fix: az network nsg rule update --nsg-name titan-hipaa-nsg -g titan-hipaa-audit-rg -n AllowSSH --source-address-prefixes 10.0.0.0/8
```

HIGH §164.312(e)(1) NIST SC-8

HTTP (80) open to internet — unencrypted web traffic

Health portal accessible over unencrypted HTTP. Patient data submitted via forms can be intercepted.

⚠ Why flagged: AllowHTTP on port 80 without corresponding HTTPS redirect. HIPAA Transmission Security requires encryption of ePHI over electronic networks.

`Fix: Delete AllowHTTP rule; only allow port 443 (HTTPS)`

CRITICAL §164.312(a)(1) PCI 1.3.4

SQL (1433) open to internet — database port exposed

Direct SQL Server access from the internet. Patient records database can be attacked with SQL injection or brute-force login attempts.

⚠ Why flagged: AllowSQL port 1433 source = *. NIST SC-7 Boundary Protection and PCI-DSS 1.3.4 require database servers not be directly accessible from untrusted networks.

`Fix: az network nsg rule delete --nsg-name titan-hipaa-nsg -g titan-hipaa-audit-rg -n AllowSQL`

SQL Server — Patient Records Database

4 FINDINGS

REAL-WORLD PRECEDENT: Montefiore Medical Center fined **$4,750,000** (2024) for insider theft of 12,500 patient records. Root cause: overly broad database access, no audit trail, no minimum necessary controls. 45 CFR §164.312(a)(1), §164.312(b), §164.514(d)

titan-hipaa-sql-west

Microsoft.Sql/servers

Location: **West US 2** Database: **PatientRecordsDB** Admin: **sqladmin**

● SQL SERVER CONFIGURATION — LIVE EVIDENCE

```
// SQL Server
{
  "name": "titan-hipaa-sql-west",
  "publicNetworkAccess": "Enabled", // database reachable from internet
```

```
  "administratorLogin": "sqladmin", // generic admin name, easily guessable
  "minimalTlsVersion": "1.2"
}

// Firewall Rules
[{ "name": "AllowAll", "startIpAddress": "0.0.0.0", "endIpAddress": "255.255.255.255" }]

// Audit Policy
{ "state": "Disabled", "retentionDays": 0 }
```

CRITICAL §164.312(a)(1) NIST AC-3

Firewall allows 0.0.0.0 – 255.255.255.255 — entire internet has access

PatientRecordsDB is accessible from any IP address on the internet. All 4.3 billion IPv4 addresses can attempt to connect.

⚠ Why flagged: Firewall rule AllowAll covers entire IP range. HIPAA Access Control requires restricting access to persons or software that have been granted access rights.

`Fix: az sql server firewall-rule delete --server titan-hipaa-sql-west -g titan-hipaa-audit-rg -n AllowAll`

CRITICAL §164.312(b) CIS 4.1.1

SQL Auditing disabled — no record of who accessed patient records

Without auditing, there is zero visibility into who queried, modified, or deleted patient data. Breach investigation is impossible.

⚠ Why flagged: audit state = Disabled. This is exactly the Montefiore scenario. HIPAA Audit Controls §164.312(b) require recording and examining activity in information systems that contain or use ePHI.

`Fix: az sql server audit-policy update --server titan-hipaa-sql-west -g titan-hipaa-audit-rg --state Enabled --storage-account titanhipaaphi`

CRITICAL §164.312(a)(1) NIST SC-7

Public network access enabled on SQL Server

SQL Server endpoint is publicly accessible. Even without the wide-open firewall rule, public network access should be disabled for ePHI databases.

⚠ Why flagged: publicNetworkAccess = Enabled. PCI-DSS 1.3 requires database servers be placed in an internal network zone.

```
Fix: az sql server update --name titan-hipaa-sql-west -g titan-hipaa-audit-rg --set publicNetworkAccess=Disabled
```

HIGH §164.308(a)(1) NIST SI-4

No Advanced Threat Protection — SQL injection attacks undetected

Without ATP, anomalous database activities (SQL injection, brute force, data exfiltration) go completely undetected.

⚠ Why flagged: No threat detection policy configured. NIST SI-4 Information System Monitoring requires automated tools to monitor for security events.

```
Fix: az sql server threat-policy update --server titan-hipaa-sql-west -g titan-hipaa-audit-rg --state Enabled
```

Virtual Network — Network Segmentation 2 FINDINGS

titan-hipaa-vnet / patient-data-subnet

Microsoft.Network/virtualNetworks/subnets

Location: **East US 2** Address Space: **10.0.0.0/16** Subnet: **10.0.1.0/24**

● SUBNET CONFIGURATION — LIVE EVIDENCE

```
{
  "name": "patient-data-subnet",
  "addressPrefix": "10.0.1.0/24",
  "networkSecurityGroup": null, // NO NSG! All traffic allowed in and out
  "serviceEndpoints": null, // no service endpoints for secure Azure access
  "privateEndpointNetworkPolicies": "Disabled"
}
```

CRITICAL §164.312(a)(1) CIS 6.5

No NSG attached to patient-data-subnet — zero network filtering

Subnet named "patient-data-subnet" has no Network Security Group. ALL traffic (any port, any protocol, any source) flows in and out unrestricted.

⚠ Why flagged: networkSecurityGroup = null. NIST SC-7 Boundary Protection requires controlling communications at the external boundary and at key internal boundaries. HITRUST 01.m requires network segregation.

```
Fix: az network vnet subnet update --name patient-data-subnet --vnet-name titan-hipaa-vnet -g titan-hipaa-audit-rg --network-security-group titan-hipaa-nsg
```

HIGH §164.312(e)(1) NIST SC-7

No service endpoints configured — Azure PaaS access over public internet

Without service endpoints, all traffic to Azure Storage and SQL flows over the public internet instead of the Azure backbone.

⚠ Why flagged: serviceEndpoints = null. PCI-DSS 1.3 requires restricting traffic between trusted and untrusted zones.

```
Fix: az network vnet subnet update --name patient-data-subnet --vnet-name titan-hipaa-vnet -g titan-hipaa-audit-rg --service-endpoints Microsoft.Storage Microsoft.Sql
```

App Service — EHR Patient Portal

5 FINDINGS

REAL-WORLD PRECEDENT: Advocate Aurora Health paid **$12,250,000** (2023) for impermissible ePHI disclosure via web tracking technologies on patient portals. NY Presbyterian Hospital fined **$300,000** by NY AG (2024). Mass General Brigham: **$18.4M**. 45 CFR §164.502(a) Impermissible Disclosure

titan-hipaa-ehr-portal

Microsoft.Web/sites

Location: **Central US** Hostname: **titan-hipaa-ehr-portal.azurewebsites.net** State: **Running**

APP SERVICE CONFIGURATION — LIVE EVIDENCE

```
// Web App Settings
{
  "name": "titan-hipaa-ehr-portal",
  "httpsOnly": false, // patients can access portal via HTTP
  "state": "Running",
  "defaultHostName": "titan-hipaa-ehr-portal.azurewebsites.net"
}

// Site Configuration
{
  "minTlsVersion": "1.0", // accepts vulnerable TLS 1.0 connections
  "ftpsState": "AllAllowed", // unencrypted FTP file transfer
  "managedServiceIdentityId": null, // no managed identity
  "ipSecurityRestrictions": "Allow" // no IP restrictions
}
```

CRITICAL §164.312(e)(1) CIS 9.2

HTTPS not enforced on patient portal

Patients accessing the EHR portal may transmit login credentials, medical records, and PII over unencrypted HTTP. One of the most common findings in OCR audits.

⚠ Why flagged: httpsOnly = false. HIPAA Transmission Security Standard requires implementing security measures to ensure ePHI is not improperly modified during transmission.

`Fix: az webapp update --name titan-hipaa-ehr-portal -g titan-hipaa-audit-rg --set httpsOnly=true`

HIGH §164.312(e)(1) PCI 4.1

TLS 1.0 allowed — deprecated, vulnerable protocol

TLS 1.0 is compromised by POODLE, BEAST, and CRIME attacks. PCI DSS removed TLS 1.0 from approved protocols in 2018.

⚠ Why flagged: minTlsVersion = 1.0. NIST SP 800-52 Rev. 2 mandates TLS 1.2 as minimum for federal systems handling sensitive data.

`Fix: az webapp config set --name titan-hipaa-ehr-portal -g titan-hipaa-audit-rg --min-tls-version 1.2`

HIGH §164.312(e)(1) CIS 9.4

FTP file transfer allowed — credentials transmitted in plaintext

Developers can upload code and configuration via unencrypted FTP. Credentials and potentially ePHI in config files are exposed.

⚠ Why flagged: ftpsState = AllAllowed. CIS 9.4 requires FTP be disabled; use FTPS or Deployment Center instead.

```
Fix: az webapp config set --name titan-hipaa-ehr-portal -g titan-hipaa-audit-rg --ftps-state Disabled
```

MEDIUM §164.312(a)(2)(i) NIST IA-2

No managed identity configured

Without managed identity, the app uses stored credentials (connection strings) to access databases and storage. Credential theft is a primary attack vector.

⚠ Why flagged: managedServiceIdentityId = null. NIST IA-2 Identification and Authentication requires unique identification of organizational users or processes.

```
Fix: az webapp identity assign --name titan-hipaa-ehr-portal -g titan-hipaa-audit-rg
```

HIGH §164.312(a)(1) NIST AC-4

No IP restrictions — admin endpoints accessible from anywhere

Management interfaces (SCM, Kudu) are accessible from any IP. Attackers who obtain deployment credentials can deploy malicious code.

⚠ Why flagged: ipSecurityRestrictions default action = Allow. SOC 2 CC6.6 requires system boundaries be monitored and access restricted.

```
Fix: Add IP restriction rules to limit access to corporate IP ranges only
```

⚠ Environment-Wide Findings 4 FINDINGS

REAL-WORLD PRECEDENT: OCR's Risk Analysis Initiative launched Oct 2024 produced **8 enforcement settlements totaling ~$900K** in its first 6 months. All targeted organizations hit by ransomware that had **no Security Risk Analysis**. 22 enforcement actions in 2024 alone, **$9.9M+** collected. 45 CFR §164.308(a)(1)(ii)(A)

titan-hipaa-audit-rg (entire environment)

Resource Group — Environment-Level Controls

Resources: **9 total** Regions: **3 (East US 2, West US 2, Central US)** Subscription: **Pay-As-You-Go**

ENVIRONMENT-LEVEL CONTROLS — MISSING

✗ Microsoft Defender for Cloud: Not enabled (Free tier)
✗ Azure Policy: No policy assignments on resource group
✗ Activity Log Alerts: No alert rules configured
✗ Diagnostic Settings: No resources have diagnostic logging
✓ Azure AD: Active (authentication present)
✓ Resource Locks: Can be applied (not currently set)

HIGH §164.308(a)(1) NIST SI-4

No Microsoft Defender for Cloud — zero threat detection

Without Defender, there is no centralized security monitoring, vulnerability assessment, or threat detection across the healthcare environment.

⚠ Why flagged: Defender plan = Free tier (no workload protection). HIPAA Security Management Process requires implementing security measures to reduce risks to ePHI.

Fix: Enable Defender for Cloud Standard plan for all resource types

MEDIUM §164.308(a)(8) NIST CM-2

No Azure Policy assignments — no configuration guardrails

Without policies, there are no automated controls preventing deployment of non-compliant resources. Anyone with access can create insecure resources.

⚠ Why flagged: Zero policy assignments on resource group. HIPAA §164.308(a)(8) requires performing periodic technical and nontechnical evaluations.

Fix: Assign built-in "HIPAA HITRUST 9.2" policy initiative to the resource group

HIGH §164.312(b) NIST AU-6

No activity log alert rules — security events go unnoticed

No alerts configured for critical operations: resource deletion, policy changes, role assignments, firewall modifications. An attacker could exfiltrate data without triggering any notification.

⚠ Why flagged: No monitor alert rules in resource group. NIST AU-6 Audit Review, Analysis, and Reporting requires reviewing and analyzing system audit records.

```
Fix: Create Activity Log Alert rules for SecurityEvent, Administrative, and Policy categories
```

MEDIUM §164.308(a)(7) NIST CP-9

No backup or disaster recovery configured

No Recovery Services Vault, no Azure Site Recovery, no automated backup policies. A ransomware attack or accidental deletion could result in permanent data loss.

⚠ Why flagged: No backup infrastructure present. HIPAA Contingency Plan §164.308(a)(7) requires data backup plan, disaster recovery plan, and emergency mode operation plan.

```
Fix: Create Recovery Services Vault and configure backup policies for SQL databases and storage accounts
```

Compliance Framework Summary

HIPAA	HITRUST CSF	NIST 800-53
24	14	22
Controls Violated	Controls Violated	Controls Violated
§164.308, §164.312	01.m, 09.m, 10.g, 12.d	AC, AU, SC, SI, IA, CM, CP

SOC 2	PCI-DSS v4	CIS AZURE
16	18	16
Controls Violated	Controls Violated	Benchmarks Failed
CC6.1, CC6.3, CC6.6, CC6.7, CC7.2	Req 1, 3, 4, 7, 8, 10, 11	Sections 3, 4, 6, 8, 9

HIPAA Violation Detail — 45 CFR Part 164

§164.312(a)(1) Access Control — 12 violations
Public access, open firewalls, no IP restrictions, no NSG

§164.312(e)(1) Transmission Security — 10 violations
HTTP allowed, TLS 1.0, FTP, no encryption in transit

§164.312(b) Audit Controls — 5 violations
No SQL auditing, no diagnostic logs, no activity alerts

§164.312(c)(1) Integrity Controls — 1 violation
Key Vault purge protection disabled

§164.308(a)(1) Security Management — 2 violations
No Defender, no threat protection

§164.308(a)(7) Contingency Plan — 1 violation
No backup or disaster recovery

Remediation Roadmap — Priority Order

#	SEVERITY	RESOURCE	FINDING	FIX COMMAND
1	CRITICAL	titan-hipaa-sql-west	Firewall allows 0.0.0.0/0	`az sql server firewall-rule delete --server titan-hipaa-sql-west -g titan-hipaa-audit-rg -n AllowAll`
2	CRITICAL	titan-hipaa-sql-west	Auditing disabled	`az sql server audit-policy update --server titan-hipaa-sql-west -g titan-hipaa-audit-rg --state Enabled`
3	CRITICAL	titan-hipaa-nsg	RDP 3389 open to internet	`az network nsg rule update --nsg-name titan-hipaa-nsg -g titan-hipaa-audit-rg -n AllowRDP --source-address-prefixes 10.0.0.0/8`
4	CRITICAL	titan-hipaa-nsg	SSH 22 open to internet	`az network nsg rule update --nsg-name titan-hipaa-nsg -g titan-hipaa-audit-rg -n AllowSSH --source-address-prefixes 10.0.0.0/8`

#	SEVERITY	RESOURCE	FINDING	FIX COMMAND
5	CRITICAL	titan-hipaa-nsg	SQL 1433 open to internet	`az network nsg rule delete --nsg-name titan-hipaa-nsg -g titan-hipaa-audit-rg -n AllowSQL`
6	CRITICAL	titanhipaaphi	HTTP allowed, no HTTPS	`az storage account update --name titanhipaaphi --https-only true`
7	CRITICAL	titanhipaaphi	Public blob access	`az storage account update --name titanhipaaphi --allow-blob-public-access false`
8	CRITICAL	titan-hipaa-kv-8842	No purge protection	`az keyvault update --name titan-hipaa-kv-8842 --enable-purge-protection true`
9	CRITICAL	titan-hipaa-ehr-portal	HTTPS not enforced	`az webapp update --name titan-hipaa-ehr-portal -g titan-hipaa-audit-rg --set httpsOnly=true`
10	CRITICAL	patient-data-subnet	No NSG attached	`az network vnet subnet update --name patient-data-subnet --vnet-name titan-hipaa-vnet -g titan-hipaa-audit-rg --nsg titan-hipaa-nsg`
11	CRITICAL	titan-hipaa-sql-west	Public network access	`az sql server update --name titan-hipaa-sql-west -g titan-hipaa-audit-rg --set publicNetworkAccess=Disabled`
12	HIGH	All resources	No diagnostic logging	`Enable diagnostic settings on all resources, send to Log Analytics workspace`

TITAN AI

Healthcare HIPAA Compliance Audit — Live Azure Scan — April 15, 2026

28 compliance violations detected across 6 frameworks • 9 Azure resources scanned • Real production environment • 0 demo data

Prepared by TITAN AI COMPLY + SENTINEL + SHADOW + AUDIT agents

titanai.tech • info@titanai.tech