COMPLIANCE · TEMPLATE

A *Minimum-Viable* HIPAA Compliance Posture for AWS

KAANSYSTEMS.COM/LIBRARY/MINIMUM-VIABLE-HIPAA-AWS · MAY 30, 2026

ABOUT THIS TEMPLATE

What 'enough' HIPAA looks like on AWS — the controls you actually need, not the 200-line compliance checklist.

THE TEMPLATE

The twelve-control map below is what the MVP posture looks like, scored against your environment. Each row gets a `yes` / `no` / `partial`. Where you have partial coverage, write a one-line note describing what's missing. The whole document fits on a page.

> ***Prefer the interactive version?*** *The HIPAA-Readiness Self-Assessment walks you through the same twelve controls in 3 minutes, computes your score, and emails you a per-category breakdown.*

#	AREA	CONTROL	SERVICE / MECHANISM
1	Legal	BAA signed	AWS Artifact
2	Legal	Only HIPAA-eligible services touch PHI	Documented list
3	Architecture	Workloads / logs / audit separated into 3+ accounts	AWS Organizations
4	Architecture	SCPs prevent CloudTrail removal	SCP `s-DenyCloudTrailDelete`
5	Identity	MFA required on all human console access	Identity Center policy
6	Identity	Root account locked + monitored	Alarm on root usage
7	Identity	Service roles least-privileged	IAM access analyzer

#	AREA	CONTROL	SERVICE / MECHANISM
8	Data	All PHI data stores encrypted at rest	KMS
9	Data	All endpoints TLS 1.2+	ELB / CloudFront / API Gateway
10	Observability	CloudTrail org-wide → log-archive account with Object Lock	CloudTrail + S3 Object Lock
11	Observability	VPC Flow Logs centralized	VPC + S3
12	Backup	Cross-region backup + annual restore drill	AWS Backup

Run through it for your environment. Anywhere you score `no`, decide one of three things: implement it this quarter, accept and document the gap, or escalate it as a compliance risk.

WHAT'S DELIBERATELY NOT HERE

The MVP skips: SIEM, intrusion detection (GuardDuty is a "should," not a "must"), Macie for PHI discovery, Web Application Firewall rules, third-party CSPM tooling. All add value. None are required for a defensible HIPAA posture on day one.

Layer them on when the audit cycle starts to feel painful. Until then, the twelve above are the work.