COMPLIANCE · TEMPLATE

Which AWS Services Are HIPAA-Eligible? The List and What It *Actually* Means

KAANSYSTEMS.COM/LIBRARY/HIPAA-ELIGIBLE-AWS-SERVICES · SEPTEMBER 16, 2026

ABOUT THIS TEMPLATE

HIPAA-eligible AWS services are the ones covered by the AWS BAA — the only services you may use for PHI. Eligibility is not compliance. What the list means.

THE TEMPLATE

The service map below is the artifact that keeps eligibility honest. List every AWS service that touches PHI — including the ones PHI reaches indirectly through logs, traces, backups, and analytics — and score each row. Anywhere a row is not clean, decide one of three things: fix it this sprint, accept and document the gap, or escalate it as a compliance risk. Keep it in your runbook and re-run it on a cadence and on every architecture change.

Prerequisite (do this first)

- [ ] AWS Business Associate Addendum (BAA) accepted in AWS Artifact
- [ ] A named owner for this map and a review cadence (quarterly, minimum)

Per-service checklist — one row per service in the PHI data path

- [ ] Service name and what PHI it touches (stored / processed / transmitted / incidental)
- [ ] Confirmed on the current AWS HIPAA-eligible-services page (date checked: _____)
- [ ] No configuration caveat — or, if there is one, we run it in the eligible configuration
- [ ] Encrypted at rest (KMS) where it holds PHI
- [ ] Enforces TLS 1.2+ in transit where it transmits PHI
- [ ] Access scoped to least privilege
- [ ] Activity logged to the tamper-proof archive

Don't-forget-these rows (PHI reaches them by accident)

- ☐ Logging / monitoring destinations (CloudWatch, and any third-party observability tool — does it have its own BAA?)
- ☐ Tracing and APM spans
- ☐ Analytics / data-warehouse pipelines fed from PHI stores
- ☐ Backup and DR targets, including cross-region copies
- ☐ Any queue, cache, or search index in the request path

Governance

- ☐ A gate exists (review step, SCP, or tagging policy) before new services are adopted in PHI-touching accounts
- ☐ The map was re-checked against the AWS list on the last review date
- ☐ Every non-clean row has a decision recorded: fix / accept-and-document / escalate

Run it once to find where PHI actually flows, then re-run it whenever the architecture moves. Eligibility is not a fact you learn once; it is a boundary you patrol.

WHAT DOES "HIPAA-ELIGIBLE" ACTUALLY MEAN?

It means AWS has placed the service in scope of the BAA — nothing more, nothing less. The BAA is the contract that makes AWS your HIPAA *business associate*: it commits AWS to handling PHI according to the Security Rule's requirements on the parts of the stack AWS controls. When AWS declares a service "HIPAA-eligible," it is saying "we will stand behind this service under the BAA." When a service is absent from the list, AWS is making no such commitment, and any PHI you put there is uncovered.

So "eligible" is a legal-coverage status, not a security rating. It does not mean the service is more secure than a non-eligible one. It does not mean the service ships in a compliant configuration. It means one specific thing: this service is inside the contract. Get that framing right and the rest of the list stops being confusing.

Two consequences follow immediately. First, you must actually sign the BAA — it is self-service in AWS Artifact, and until you accept it, *none* of your services are covered, eligible or otherwise. Second, the BAA extends only to the eligible services, so the coverage you just signed for evaporates the moment PHI flows into a service that is not on the list.