Palo Alto Health Labs

HIPAA-Ready Hosting and Database Selection Guide

Not legal advice. Not a compliance certification.

"HIPAA-ready" describes a selection and configuration goal here, not a guarantee. HHS permits covered cloud use with an appropriate BAA and other applicable HIPAA obligations, including risk analysis and risk management. A vendor offering an agreement is not evidence that your organization has executed it or configured the right services. [1]

Project/version: _____ Review date: _____
Workflow/data classes, without patient examples: _____
Technical owner: _____ Agreement/scope reviewer: _____

1. Define the boundary before comparing providers

Map runtime, database, file storage, backups, logs, support and model calls separately. A coding tool, hosted application and external database are distinct review targets. Record the exact legal vendor, product, account/project, plan/add-on and data received for each.

HHS explains that storing encrypted ePHI can still make a cloud provider a business associate even without the decryption key. Encryption is not a substitute for analyzing the contractual relationship. [1]

2. Public eligibility examples — not endorsements

Verified on means public documentation was opened/read on the stated date; no customer coverage was verified.

Product boundary	Documented pathway	Remaining checks	Official source / verified on
Vercel deployment infrastructure	BAA available conditionally to Pro with HIPAA add-on, or Enterprise through account team.	Executed agreement, exact services/configuration, separate database/model relationships; do not infer coding-tool coverage.	Vercel guide <https://vercel.com/kb/guide/hipaa-compliance-guide-vercel>, 2026-11-07 PST
AWS HIPAA-eligible services	Standard BAA through AWS Artifact; PHI processing/storage/transmission limited to eligible services under agreement.	Account coverage and exact current service eligibility; not all AWS services are eligible merely because an account has a BAA.	AWS FAQ <https://aws.amazon.com/compliance/hipaa-compliance/>, 2026-11-07 PST

Product boundary	Documented pathway	Remaining checks	Official source / verified on
Supabase designated HIPAA projects	Available, conditional: legal BAA Version 1 (October 23, 2026) §14 requires no signature. Acceptance of the Agreement AND subscription to the HIPAA Add-On constitutes customer acceptance; Supabase accepts by making the BAA available and providing the add-on. Effective on first add-on subscription; binding only with that subscription unless otherwise agreed in writing. Applies only where the customer is a covered entity or business associate and Supabase acts as its business associate; remains effective while the add-on and Agreement remain active.	Confirm current plan eligibility, exact Services, governing terms and acceptance record; the legal BAA does not establish Team-plan eligibility. Project docs still say "signed BAA"; retain this documentation discrepancy for account-specific confirmation. Configure High Compliance and apply healthcare responsibilities including MFA, recovery, SSL enforcement, network restrictions and connection logging. Dashboard AI/MCP and third-party coverage is not established here.	Legal BAA, opening terms and §§3, 11, 14 <https://supabase.com/legal/customer-resources/business-associate-agreement>; HIPAA projects <https://supabase.com/docs/guides/platform/hipaa-projects>; responsibilities <https://supabase.com/docs/guides/deployment/shared-responsibility-model>; reviewed 2026-11-07 PST

Supabase plan eligibility is intentionally a customer check in this guide; its project page alone does not establish every plan condition. These examples are not exhaustive. If another provider's public documents are silent, mark Unknown, not No.

3. Complete one comparison per candidate

Candidate/exact product: _____ Account/project: _____
Public BAA pathway: Available / Explicitly restricted / Unknown
Evidence URL and date: _____
Eligible plan/add-on/services: _____
Executed agreement evidence reference and reviewer: _____
Covered environments/features and exclusions: _____
Retention, regions, deletion/export terms: _____
Provider responsibilities: _____
Customer responsibilities and named owner: _____

4. Require operational evidence, not just features

Mark Demonstrated / Open / Not applicable with reason.

Proposed acceptance question	Status / evidence	Owner
Can access roles and denied record/tenant access be tested?		
Can privileged accounts and credential rotation be governed?		
Are encryption and network controls documented/configured?		

Proposed acceptance question	Status / evidence	Owner
Do logs support investigation without uncontrolled patient-content copies?		
Can backups actually be restored and reconciled?		
Are patching, availability and incident escalation assigned?		
Can data be returned/exported and residual copies addressed at exit?		

These are proposed implementation checks, not a complete HIPAA checklist. HHS discusses availability, backup/recovery, access, retention and shared cloud responsibilities; its Security Rule summary describes administrative, physical and technical safeguards. [1][2]

5. Record a conditional selection

Preferred candidate and reason: _____
Blocking evidence/contract/configuration gaps: _____
Interim restriction while unresolved: _____
Next action / owner / due: _____
Organization decision reviewer / date: _____
Recheck trigger: New service / Feature / Region / Model / Agreement change

Do not introduce real patient data to an unresolved processing path. A shortlist is not a release decision or compliance certificate.

Source/editorial appendix

All sources opened/read 2026-11-07 PST. Vendor rows are public-document findings only; no account, signed BAA or private eligible-service configuration was reviewed.

[1] HHS cloud guidance <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html>.
[2] HHS Security Rule summary <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>.

Mike: review service-boundary wording and “HIPAA-ready” framing. Reviewer should verify exact contracted service, plan and feature eligibility before any deployment. No pricing or vendor rankings included.

Limits

No PAHL capability, certification, outcome or delivery promise is asserted.

Not legal advice.

No booking URL, availability or free-call deliverables have been verified.