Palo Alto Health Labs

The 2026 BAA Matrix — Printable Reference Copy

Not legal advice. Not a compliance certification.

Use this selected-stack reference to identify questions for a service-specific agreement review, not to authorize PHI use. BAA availability is not signed coverage, and a BAA alone does not make an app compliant.

Status legend and verification boundary

Available, conditional = public documentation describes an agreement pathway, subject to customer eligibility/configuration and executed terms. Explicit restriction = a reviewed source actually excludes the use. UNCONFIRMED = the reviewed source does not establish status; it does not mean No. Dates record public-source review on 2026-11-07 PST, not contract acceptance or validation of an installation.

Reference matrix — exact reuse from article 5

Category	Vendor / product boundary	Public status / plan / add-on	Unresolved customer checks	Official source	Verified on
Builders / coding	Lovable hosted builder	Explicit restriction: Enterprise FAQ says no current BAAs and no PHI uploads.	External hosting of generated code does not authorize PHI in builder prompts.	Enterprise FAQ <https://docs.lovable.dev/introduction/lovable-for-enterprise>	2026-11-07 PST
Builders / coding	Replit Agent, workspace and published apps	UNCONFIRMED: reviewed shared-responsibility page does not establish BAA availability, eligible plan or service.	Customer responsibility for application HIPAA compliance does not prove the vendor refuses BAAs. Written clarification needed.	Shared responsibility <https://docs.replit.com/features/security/shared-responsibility-model>	2026-11-07 PST — source read; BAA status not verified
Builders / coding	Bolt.new hosted builder versus own-cloud BYOK	UNCONFIRMED: security page describes own AWS/Azure tenant deployment but does not establish hosted-builder BAA availability or contractual scope.	Confirm plan, agreement, meaning of BYOK, and external prompt/model/control-plane processing. Own-cloud marketing is not signed coverage.	Security <https://bolt.new/platform/security>	2026-11-07 PST — source read; BAA status not verified
Builders / coding	Vercel v0 AI Solution / v0 API	Explicit restriction: API Terms §5.4 prohibit processing PHI in the v0 API or AI Solution.	Separate from hosting; do not infer permission from a Vercel infrastructure BAA. Review negotiated terms separately.	API Terms <https://vercel.com/legal/api-terms>	2026-11-07 PST
Builders / coding	Cursor Enterprise eligible services	Available, conditional: Enterprise agreement and signed BAA; locked organization-wide Privacy Mode and Eligible Services/Models required.	Private HIPAA Guide governs current scope/configuration; third parties are not automatically covered. Coding service, not app hosting.	BAA docs <https://cursor.com/docs/enterprise/baa>	2026-11-07 PST — public page only

Category	Vendor / product boundary	Public status / plan / add-on	Unresolved customer checks	Official source	Verified on
Hosts	Vercel deployment infrastructure	Available, conditional: Pro with HIPAA add-on or Enterprise through account team.	Obtain executed BAA and confirm exact enabled services. Database/model integrations remain separate; v0 is not authorized by this row.	HIPAA guide <https://vercel.com/kb/guide/hipaa-compliance-guide-vercel>	2026-11-07 PST
Hosts	AWS HIPAA-eligible cloud services	Available, conditional: standard BAA through AWS Artifact; PHI only in HIPAA-eligible services under the agreement.	Confirm account coverage and current eligible-service list for each component; not blanket permission for every AWS service.	HIPAA FAQ <https://aws.amazon.com/compliance/hipaa-compliance/>	2026-11-07 PST
Databases	Supabase managed platform / designated 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>	2026-11-07 PST
Models / APIs and chat	OpenAI API eligible functionality	Available, conditional: eligible organizations can accept standard BAA in API Platform; enterprise agreement not required. Executed BAA plus Modified Retention required unless OpenAI specifies otherwise.	Check organization eligibility, endpoint, model/feature and HIPAA Guide configuration. An API key alone proves no coverage.	API enrollment <https://help.openai.com/en/articles/8660679-how-can-i-get-a-business-associate-agreement-baa-with-openai>; eligibility <https://help.openai.com/en/articles/20001069>	2026-11-07 PST

Category	Vendor / product boundary	Public status / plan / add-on	Unresolved customer checks	Official source	Verified on
Models / APIs and chat	OpenAI ChatGPT eligible workspaces versus Business / consumer app	Product-specific: eligibility page lists Healthcare, Enterprise with Regulated Workspace, FedRAMP and Clinicians. Enrollment page explicitly says no BAA for Business.	Confirm signed product and feature scope. Enterprise/Edu sales-contact language is not blanket coverage. Free/Plus coverage not established by reviewed pages; consumer PHI permission is not inferred.	Eligibility <https://help.openai.com/en/articles/20001069>; BAA enrollment / ChatGPT section <https://help.openai.com/en/articles/8660679-how-can-i-get-a-business-associate-agreement-baa-with-openai>	2026-11-07 PST — consumer coverage unconfirmed

Customer coverage worksheet

Project/version: _____ Review date: _____
Chosen vendor/product: _____ Account/project: _____
Plan/add-on: _____ Intended processing: _____
Executed agreement evidence reference: _____
Covered service/feature and retention evidence: _____
Excluded features/connectors: _____
Configuration evidence: _____ Reviewer/owner: _____
Unresolved question: _____ Next check/date: _____
Decision: No PHI in unresolved workflow / Review completed by accountable organization / Pause.

Complete a separate worksheet per service boundary. Do not attach contracts, credentials or patient examples to a public form. Agreement availability and exact customer coverage must remain separate fields.

Source limitations and follow-up

Replit and Bolt BAA status remains unconfirmed. Cursor's private HIPAA Guide was not inspected. OpenAI's current enrollment and eligibility pages describe different product/configuration boundaries; do not flatten these into a vendor-wide Yes. All accounts, negotiated terms, exact model eligibility and institutional approvals remain unverified.

HHS cloud guidance <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html>, opened/read 2026-11-07 PST, supplies the general regulatory framing. Row-level official sources and verification dates are preserved above. Recheck on publication day and before procurement decisions.

Limits

Checkboxes and decision gates are proposed practices, not a complete legal checklist, clinical validation instrument or compliance certification.

No PAHL delivery capability or client outcome is asserted.

Do not enter patient identifiers, PHI, credentials or access tokens in these worksheets; use system labels and approved evidence references instead.

Not legal advice.

Do not invent a booking URL, availability or deliverables for the free call.