Palo Alto Health Labs

The Vibe-Coded App HIPAA Readiness Checklist

Not legal advice. Not a compliance certification.

Use this worksheet to organize open questions before moving a prototype into a patient-data workflow. “Complete” means evidence is recorded, not that the application has passed an external assessment.

Project label: _____ Version: _____ Review date: _____
Intended user/task: _____
Excluded uses: _____
Accountable product owner: _____ Technical owner: _____
Clinical reviewer, if applicable: _____ Legal/security reviewer: _____

For each item mark Done / Open / Not applicable, add an evidence reference and name the person responsible. Explain every Not applicable. Do not total a readiness score.

1. Scope and data

☐ State the business arrangement and obtain a determination of applicable HIPAA roles; do not infer scope solely from a physician's involvement.

☐ Identify data created, received, stored and transmitted, including uploads, backups, telemetry and support channels.

☐ Separate synthetic-data development from approved production processing.

☐ Record each external destination and its retention/deletion behavior.

Evidence references / unresolved scope / owner: _____

2. Agreements and service boundaries

☐ List the legal entity, exact product, account/project, plan and add-on for each provider.

☐ Where required, record executed BAA evidence and covered service/functionality—not merely a vendor's offer to sign.

☐ Resolve model endpoints, connectors, logging and support exclusions before using PHI there.

☐ Keep unresolved vendor status marked Unknown; do not convert missing documentation into No.

Evidence references / unresolved services / owner: _____

3. Access and implementation

☐ Define user roles and test denied access, including another user's/tenant's records.

☐ Keep secrets out of client bundles and coding prompts; rehearse rotation.

☐ Review administrator authentication and privileged access.

☐ Test uploads, exports, caches and logging paths for unintended disclosures.

☐ Document dependencies, configuration and reproducible deployment.

Evidence references / failed tests / owner: _____

4. Operations and clinical workflow

☐ Exercise backup restoration and document a recovery decision owner.

☐ Define monitoring, incident escalation, access review and maintenance ownership.

☐ Specify source freshness, missing-data behavior and downtime alternatives.

☐ For generated clinical content, propose visible draft status and accountable acceptance rather than automatic action.

☐ For EHR connections, verify supported operations and environment-specific permissions; rehearse context switches and failed requests.

Evidence references / acceptance gaps / owner: _____

5. Decision record

Choose: Continue synthetic-data evaluation / Remediate and reassess / Request organization review / Pause.
Reason and blocking issues: _____
Next action: _____ Owner: _____ Due: _____
Review decision and evidence reference: _____

Do not interpret all checked boxes as a release authorization. HHS pairs appropriate cloud BAAs with other HIPAA duties, including risk analysis and risk management.

Sources

- 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: scope, cloud agreements, risk analysis and recovery responsibilities.
- HL7 FHIR R4 security <https://hl7.org/fhir/R4/security.html>, opened/read 2026-11-07 PST: authentication, authorization, logging and implementer responsibilities.

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.