Palo Alto Health Labs

Is your app HIPAA-ready? 15-question self-assessment

Not legal advice. Not a compliance certification.

Not legal advice or launch approval.

Downloadable Markdown master

Instructions and evidence boundaries

Work on one defined workflow and version at a time. Use a neutral internal project alias, environment description, review date, and reviewer roles—not personal contact details or patient identifiers. Record evidence references in an approved internal repository; do not attach production records.

For each numbered question choose **documented / needs review / unknown / not applicable**. Add the reviewer's rationale, evidence reference and date, unresolved gap, responsible role, and next action. “Documented” means an artifact exists, not that its adequacy has been established. “Not applicable” requires a reason and reviewer review; it is not a shortcut around a duty. Do not total responses or convert them into a readiness threshold, penalty tier, fine estimate, or automated decision.

Do not enter actual PHI, names, identifiers, secrets, credentials, production screenshots, payloads, logs, or records. Use MOCK/SYNTHETIC examples only. References should point to restricted evidence without reproducing its contents or exposing access links outside the authorized team.

How to read the prompts: “Obligation, if applicable” summarizes a sourced legal requirement for the regulated role and activity. “Implementation recommendation” describes a suggested evidence-gathering or engineering method, not mandated technology. The current Security Rule distinguishes required and addressable implementation specifications; addressable does not mean optional without assessment and documentation. Neither MFA nor row-level security (RLS) is presented here as a blanket mandate; implementation depends on applicable requirements, risk analysis, architecture, and contractual scope. §164.306 and technical safeguards <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.

1. Which operator, role, and activity have reviewers assessed for HIPAA applicability?

Obligation, if applicable: HIPAA applies to covered entities and business associates; being a physician or calling a tool a health app does not alone settle the role analysis. Provider coverage depends on specified electronic standard transactions. HHS applicability <https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html>.

Implementation recommendation: record the legal/privacy review reference, workforce versus vendor relationship, intended users, and unresolved scope questions. Route other-law questions to counsel; an out-of-scope HIPAA conclusion is not general privacy clearance.

2. What evidence maps the information the workflow creates, receives, maintains, and transmits?

Obligation, if applicable: risk analysis covers potential risks and vulnerabilities to all ePHI held by the regulated entity. §164.308(a)(1) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.

Implementation recommendation: reference a data-category and purpose inventory, including intake, exports, retention, deletion, and backups. Record classification uncertainty without inserting actual records.

3. Where could information reach prompts, logs, previews, analytics, or support tools?

Implementation recommendation: map development and runtime paths separately, including model endpoints, error traces, URLs, browser storage, test copies, and integrations. Cite sanitized configuration reviews and MOCK/SYNTHETIC observations. A production database diagram alone is insufficient evidence for this inventory.

4. Which exact services and activities have applicable BAA coverage and shared responsibilities documented?

Obligation, if applicable: a cloud provider handling ePHI on behalf of a covered entity or business associate can itself be a business associate, including encrypted no-view storage; a BAA does not replace the customer's other obligations. HHS cloud guidance, introduction and Q1–2 <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html>.

Implementation recommendation: reference accepted agreements, legal entities, service schedules, account/project boundaries, model features, exclusions, subcontractor review, and customer configuration responsibilities. Do not infer coverage from a brand, badge, or unrelated hosting agreement.

5. What evidence supports the permitted purposes and disclosures of this workflow?

Obligation, if applicable: business associates may use and disclose PHI only as permitted by their BAA and the Privacy Rule or as required by law. HHS cloud guidance, Privacy Rule considerations <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html>.

Implementation recommendation: record privacy review of sharing, exports, notices, and individual-rights workflows; flag unresolved permission questions rather than treating a settings toggle as authorization.

6. How are user and service identities verified and access changes controlled?

Obligation, if applicable: the Security Rule includes unique user identification, person/entity authentication, and access controls. §164.312(a), (d) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.

Implementation recommendation: reference joiner/leaver procedures, session review, service-identity ownership, emergency access, and privileged-access evidence. Record MFA decisions and vendor conditions without assuming one technology establishes compliance.

7. What tests demonstrate server-side authorization and separation between users or organizations?

Implementation recommendation: reference MOCK/SYNTHETIC negative tests for direct API requests, record identifiers, exports, files, and elevated roles. Test beyond hidden interface buttons. RLS may be one implementation technique, not a universal architecture requirement or substitute for application authorization review.

8. Where are the risk analysis, risk-management actions, and accountable security role documented?

Obligation, if applicable: risk analysis and risk management are required implementation specifications, and a security official must be identified. §164.308(a)(1)–(2) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.

Implementation recommendation: reference a current assessment, action owners, review dates, and unresolved findings across people, systems, and vendors. Do not replace that assessment with this worksheet.

9. What evidence supports technical safeguards and ongoing activity review?

Obligation, if applicable: technical standards include audit controls, integrity, authentication, and transmission security; administrative requirements include system-activity review. Addressable encryption specifications require the §164.306 assessment process, not casual omission. §§164.306, 164.308(a)(1), 164.312 <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.

Implementation recommendation: reference safeguard decisions, key-management ownership, patch review, monitoring responsibilities, and sanitized test evidence. Keep sensitive logs elsewhere.

10. How are workstations, facilities, devices, and media protected through disposal or reuse?

Obligation, if applicable: physical safeguards cover facility access, workstation use/security, and device/media controls, including disposal and reuse. §164.310 <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.

Implementation recommendation: reference policies and operational checks for clinic devices, remote work, removable media, and discarded equipment; do not limit review to cloud settings.

11. What evidence shows workforce procedures are implemented rather than merely written?

Obligation, if applicable: the Security Rule includes workforce security, security awareness/training, and policies with documentation requirements. §§164.308(a)(3), (5), 164.316 <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.

Implementation recommendation: reference training records, role-based access reviews, policy ownership, and offboarding checks without listing individual staff details here.

12. Who handles suspected incidents and assesses breach-notification obligations promptly?

Obligation, if applicable: incident response and HIPAA breach notification are related but distinct duties; notification follows breaches of unsecured PHI subject to the rule's definitions and exceptions. §164.308(a)(6) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>; HHS breach guidance <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>.

Implementation recommendation: reference escalation procedures, discovery-time recording, evidence preservation, legal review, vendor reporting, and notice ownership. Suspected incidents go to responsible responders immediately, not into a booking queue or this worksheet.

13. What evidence supports backup, recovery, and emergency operations?

Obligation, if applicable: contingency planning includes required backup, disaster-recovery, and emergency-mode procedures; testing/revision is addressable under the rule's assessment framework. §164.308(a)(7) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.

Implementation recommendation: reference restore exercises, recovery ownership, dependency outages, and manual fallback rehearsals using synthetic fixtures rather than placing real backup contents here.

14. What separate clinical-safety review supports the intended use and limits?

Implementation recommendation: document qualified clinical review of intended users, foreseeable misuse, incorrect outputs, escalation, downtime, human oversight, and change effects. Identify unresolved clinical and regulatory questions for appropriate reviewers. Clinical-safety evidence is separate from HIPAA review; neither establishes the other or authorizes launch.

15. How will unresolved gaps and future changes receive accountable review?

Obligation, if applicable: regulated entities must evaluate security measures and maintain/update required policies and documentation as applicable conditions change. §§164.306(e), 164.308(a)(8), 164.316 <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.

Implementation recommendation: keep an open-action register with responsible roles, evidence needed, review dates, and affected workflows. Route release decisions through the organization's authorized legal, security, operational, and clinical governance—not through a response count.

Using the evidence register

Group the resulting gaps by responsible reviewer and agree next actions through approved internal processes. Leave uncertain items visible. An introductory discussion can start with a synthetic workflow description and a non-sensitive summary of open questions; do not transmit the register or restricted evidence unless a separately approved secure process exists.

Book a free 30-minute audit

The proposed call is an introductory discussion, not a completed compliance audit, legal determination, certification, or clinical-safety review. Booking does not replace urgent incident response.

Limits

No PAHL compliance status, BAA availability, clinical-review capacity, deliverables, or outcome guarantee asserted.

No scores, numeric risk, penalty outputs, certification, or all-documented inference.