Palo Alto Health Labs

Vibe-coded app risk analysis starter

Not legal advice. Not a compliance certification.

Not legal advice or launch clearance.

Foundation and optional SRA resource

Section 164.308(a)(1)(ii)(A) requires an accurate and thorough assessment of potential risks and vulnerabilities to ePHI confidentiality, integrity, and availability. Subsection (B) separately requires risk management: implementing measures sufficient to reduce risks/vulnerabilities to a reasonable and appropriate level. An inventory is input to analysis; an action list is not proof that risk-management measures were implemented. §164.308(a)(1)(ii)(A)–(B) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.308>.

OCR guidance includes scope/data collection, documented threats/vulnerabilities, existing security measures, likelihood, potential impact, risk-level determination, documentation, and ongoing review. **Likelihood and impact evaluation are elements of the actual analysis, but are deliberately not performed or scored here.** No quantitative or qualitative risk ratings, probabilities, color matrices, automated priorities, or compliance verdicts belong in this starter. A qualified reviewer must complete the missing evaluation across the full organizational ePHI scope. OCR risk-analysis guidance, Elements of a Risk Analysis <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>.

The live ONC SRA Tool page currently lists **version 3.7** for its Windows application and Excel workbook and identifies its v3.7 user guide; the page states **last updated September 18, 2026**. The listed audience is small/medium providers. Its workbook includes formulas and conditional formatting to calculate/help identify risk; **this worksheet intentionally does not reproduce that scoring or formatting**. The official page says tool use is not required and does not guarantee compliance, and that it is not exhaustive or definitive. Version statements here describe the page opened, not an installed or tested product. No software/workbook was downloaded or run. ONC SRA Tool page <https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool>.

Worksheet 1 — Scope, roles, and review boundaries

Use generic roles and neutral reference codes only; no patient identifiers, actual clinical narratives, production records/logs, screenshots, secrets, credentials, or patient-bearing URLs. Do not upload evidence here or in booking. Real underlying records stay in approved restricted systems. Use MOCK/SYNTHETIC fixtures for examples; do not assume this worksheet is privileged.

Project alias _____ / version/environment _____ / inventory date and zone _____

Operator role proposed: covered entity / business associate / subcontractor / other / unknown _____

Applicability-review role and rationale reference _____

Workflow purpose and intended actor roles _____

In-scope environments/locations, including remote workforce _____

Excluded or unknown dependencies and reason for further review _____

Qualified review owner / full-organization scope reference / handoff action _____

The Security Rule obligations concern covered entities/business associates and all ePHI they create, receive, maintain, or transmit. Scope must not stop at a production database or a single location. Document what remains outside this app inventory for wider review. §164.306(a) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.306>; OCR guidance, Scope and Data Collection <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>.

Worksheet 2 — PHI/ePHI flow boundaries

For every applicable row use the companion record beneath the table. “None expected” is a proposed design statement to verify, not proof no data reaches the destination. Keep unknown paths visible.

Boundary code	Inventory prompt	Flow-record reference
BUILD	Builder, code-generation prompts, attachments, chat history	___
DEV	Repository, build jobs, previews, test fixtures, developer machines	___
ID	Production identity, sessions, service accounts, privileged access	___
API	Browser/client, APIs, server-side authorization, integrations	___
STORE	Database, files, caches, exports, temporary storage	___
MODEL	Model gateways/endpoints, accounts, retained inputs/outputs	___
RECOVER	Backups, replicas, recovery copies, restore environment	___
OBSERVE	Telemetry, error traces, analytics, URLs, support systems	___
PEOPLE	Workforce workflows, remote work, devices, physical locations	___
VENDOR	Vendor/subcontractor services and onward recipients	___

Repeatable flow record

Flow code _____ / generic information category and proposed PHI/ePHI status _____

Source → destination (neutral system aliases) _____

Actor roles / purpose / creates, receives, maintains, transmits (identify all applicable) _____

Environment/location category / copy lifecycle / access boundary _____

Responsible customer/vendor/subcontractor roles _____

Agreement acceptance / covered service-account-feature scope / exclusions reference _____

Sanitized evidence reference/date / unknowns / owner role / next action _____

These are suggested inventory fields, not a universally mandated diagram format. OCR guidance calls for identifying and documenting where ePHI is stored, received, maintained, or transmitted. OCR guidance, Data Collection <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>.

A cloud host maintaining encrypted ePHI on a regulated entity's behalf can still be a business associate without holding the key. No-view storage is not a blanket exemption, and a BAA does not replace other applicable duties. Record actual responsibilities and covered service scope rather than assuming coverage from a vendor name. HHS cloud guidance, introduction and Q1–2 <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html>.

Worksheet 3 — Threat, vulnerability, and safeguard: keep them separate

OCR guidance describes threats as potential sources/events that can exercise a weakness, and vulnerabilities as flaws/weaknesses in procedures, design, implementation, or internal controls. Administrative and physical weaknesses belong alongside technical ones. The examples below are invented teaching examples, **MOCK/SYNTHETIC—not actual incidents or findings**. OCR guidance, Important Definitions <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>.

MOCK/SYNTHETIC threat source/event	Distinct hypothetical vulnerability	Proposed safeguard to examine, not proof implemented
Test user attempts cross-account access	Test API trusts a client-supplied account label	Server-side authorization checks and negative synthetic tests
Invented staff member inadvertently includes a test record in support	Unclear escalation procedure and broad support export access	Workforce instructions, limited export paths, and access review
Simulated water leak near a test workstation	Equipment placed in an exposed location with no reviewed protection	Physical protection and continuity arrangements
Simulated service outage	Restore procedure has not been exercised in the test environment	Recovery procedure and authorized synthetic restore exercise

Repeatable observation record

Observation code / linked flow codes _____

Potential threat source (human/natural/environmental) and event _____

Specific vulnerability or knowledge gap _____

Possible confidentiality/integrity/availability effect described factually, without magnitude or rating _____

Existing safeguard / policy reference _____

Evidence of actual operation/configuration, reference and date _____

Implementation status: reported present / evidence available for review / planned / unknown / not applicable with rationale _____

What evidence does not establish / remaining gap _____

Owner role / next evidence-gathering action _____

Do not treat “evidence available” as adequate control verification. No estimates of likelihood, impact level, risk level, or relative priority should be entered. Those belong to the qualified full analysis, outside this starter.

Worksheet 4 — Safeguard coverage and applicability

The rule addresses administrative, physical, and technical safeguards, with required and addressable implementation specifications. Required specifications must be implemented where applicable. Addressable does not mean optional: assess whether reasonable/appropriate; implement when it is, otherwise document why not and implement an equivalent alternative if reasonable/appropriate. This inventory does not perform that decision. §164.306(c)–(d) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.306>.

Coverage area	Suggested evidence topics for qualified review	Reference / gap / owner role
Administrative	Risk-analysis scope, workforce access changes/training, activity review, incident procedures, contingency ownership, evaluation	___ / ___ / ___
Physical	Facilities, remote workstations, device/media handling and authorized access	___ / ___ / ___
Technical	Identity/authentication, server authorization, audit controls, integrity and transmission protections	___ / ___ / ___
Organizational/vendor	Service responsibilities, accepted agreements, subcontractor chain and evidence boundaries	___ / ___ / ___
Required/addressable review	Applicable specification, reviewer rationale, decision/equivalent-measure documentation reference still needed	___ / ___ / ___

The table lists preparation topics, not named mandatory documents or a complete control list. No blanket MFA/RLS architecture mandate, annual review schedule, or retention period is asserted. Review/update needs depend on circumstances and changes; OCR guidance says the rule does not prescribe a single risk-analysis frequency. §164.306(e) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.306>; §164.308(a)(8) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.308>; OCR guidance, Periodic Review <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>.

Worksheet 5 — Separate risk-management handoff

Use this register only for proposed actions or evidence requests. It is not an approved risk-management plan, automated ordering system, or accepted-residual-risk decision. Risk management requires implementation, not just an inventory of intentions. §164.308(a)(1)(ii)(B) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.308>.

Observation / evidence gap code	Proposed action or reviewer question	Responsible role	Dependency / next review trigger	Evidence needed to verify implementation
___	___	___	___	___
___	___	___	___	___

Worksheet 6 — Qualified-review handoff and open questions

Full ePHI environments/locations not yet covered _____

Unverified flows, vendor/subcontractor responsibilities, and evidence gaps _____

Qualified reviewer role / scope reference / next action _____

Remaining work: full scope reconciliation, likelihood/impact evaluation and risk determination, adequate documented analysis, and risk-management decisions/implementation. No ratings are supplied or requested in this starter. OCR guidance, Elements and Finalize Documentation <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>.

Review triggers to discuss: new integrations/models, changing data use or hosting, workforce/operational changes, and suspected incidents. Preserve evidence and escalate incidents promptly rather than waiting to complete analysis. OCR guidance, Periodic Review <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>; §164.308(a)(6), (8) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.308>.

Official sources and internal editorial holds

All sources opened November 7, 2026 (PST):

- ONC Security Risk Assessment Tool page <https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool> — live page lists v3.7, application/workbook/user guide; September 18, 2026 update date. No binaries, workbook internals, or user-guide PDF independently inspected.
- HHS OCR Guidance on Risk Analysis <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html> — scope, collection, threat/vulnerability definitions, measures, likelihood/impact, risk determination, documentation and updates; page reviewed August 12, 2026.
- 45 CFR 164.308 <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.308> — risk analysis/management and related administrative safeguards.
- 45 CFR 164.306 <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.306> — scope, flexibility, required/addressable distinctions and maintenance.
- HHS HIPAA and Cloud Computing <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html> — no-view BA status and shared responsibilities.

No PAHL compliance, BAA availability, capability, emergency response, deliverable, or prevention guarantee asserted.

An introductory discussion is not a completed risk analysis or compliance audit. Share only a generic non-sensitive description of open questions; no actual records or patient details in booking.

Book a free 30-minute audit