Palo Alto Health Labs

Suspected breach in your vibe-coded app: first-response checklist

Not legal advice. Not a compliance certification.

Act now if an incident is suspected: contact responsible incident responders and privacy/security leadership promptly, involving counsel as appropriate. Do not wait for worksheet completion, confirmed impact, or a booking. Coordinate safe containment, evidence preservation, and clinical continuity rather than investigating on your own.

Not legal advice or an emergency-response service.

Printable first-response checklist

Use generic owner roles and neutral reference codes only. Each checkbox means an action is assigned or tracked—not compliance approval. For each item record: status _____ / owner role _____ / evidence reference _____ / next action _____.

Do not enter patient details, identifiers, clinical narratives, secrets, credentials, production log dumps, screenshots, or actual evidence here or in booking notes. Keep real evidence in authorized restricted systems and use verified, approved response channels. Use MOCK/SYNTHETIC examples only. This worksheet does not establish or promise legal privilege.

☐ **1. Escalate and assign coordination.** Notify designated responders and privacy/security leadership; identify counsel and clinical-operations roles. Record an internal incident-reference code, not sensitive facts. Security incident response includes suspected or known incidents; do not wait for a reportable-breach conclusion. HHS/FTC joint guidance, Security Rule safeguards <https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-ftc-act/index.html>.

☐ **2. Contain safely while preserving evidence.** Have authorized responders restrict ongoing unauthorized transmissions/access and arrange an approved clinical alternative. Coordinate any isolation, access changes, credential changes, or service interruption with evidence collection and patient-safety needs. No blanket power-off, wipe, delete, or rotation instruction is appropriate here. Do not erase logs, chats, accounts, or historical configuration to hide the problem.

☐ **3. Preserve the factual record.** Through approved procedures preserve relevant original correspondence, configurations, routing/account scope, audit evidence, policy versions, and response actions. Track source/version/date and custodian role in the restricted response record. Distinguish contemporaneous evidence from later remediation; never backdate or alter missing records. Do not probe other patients' records or reproduce the issue against production data without authorization.

☐ **4. Establish roles, data, and paths.** Have legal/privacy reviewers determine HIPAA covered-entity/business-associate status, possible PHI, and separate consumer-app applicability. Inventory builder, preview, host, database, model endpoint, telemetry, support, exports, backups, and onward recipients using generic categories here. HIPAA and FTC HBNR have distinct coverage tests; a consumer-facing feature alone settles neither. Joint guidance <https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-ftc-act/index.html>; §318.1–.2 <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318>.

☐ **5. Record discovery candidates immediately.** Preserve earliest alerts, who knew or reasonably should have known, their role/agency relationship, event times and zones, and uncertainties. Counsel determines the legally relevant discovery date; do not reset it to confirmation, management approval, worksheet completion, or booking. See discovery rules below. §164.404(a)(2), §164.410(a)(2) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>; §318.3(c) <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318>.

☐ **6. Assign the correct assessment.** For HIPAA, distinguish suspected incident, impermissible use/disclosure, and reportable breach of unsecured PHI; examine exceptions, secured status, and the assessment below. For FTC HBNR, use its own definitions and unauthorized-acquisition presumption—not HIPAA's four-factor test. Keep unknown facts visible. §164.402 <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>; §318.2 <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318>.

☐ **7. Assign notification and contract review now.** Identify applicable individuals, regulator, media, customer/vendor, state, and contractual obligations. Review notice methods, content, substitute notice, and authorized senders with counsel; the tables are not an exhaustive operational notice template. Earlier state/contract duties may apply; assess rather than assume the federal outside limit controls everything. §§164.404–.410 <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>; §§318.3–.6 <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318>.

☐ **8. Track decisions and continue response.** Maintain restricted assessment rationale, authorized remediation, delivery/reporting evidence, unresolved gaps, and next review. The applicable HIPAA entity bears proof of required notification or why an impermissible use/disclosure was not a breach; FTC entities bear proof of required notices and necessity of delay. Neither a blank log nor completion of this sheet is a breach determination or launch clearance. §164.414(b) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>; §318.4(c) <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318>.

HIPAA assessment: no numeric score

An impermissible acquisition, access, use, or disclosure is presumed a breach unless a specified exception applies or the applicable covered entity/business associate demonstrates low probability of compromise through a risk assessment covering at least these four factors. Record the detailed analysis securely; enter only reviewer-role and evidence codes here. §164.402, breach definition (1)–(2) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>.

Factor	Restricted assessment should address	Reviewer role / reference
Nature and extent	Information involved, identifier types, likelihood of re-identification. §164.402(2)(i) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>.	___ / ___
Unauthorized person	Who used or received the information and relevant circumstances. §164.402(2)(ii) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>.	___ / ___
Actual acquisition/viewing	Evidence whether information was actually acquired or viewed; missing evidence remains uncertainty. §164.402(2)(iii) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>.	___ / ___
Mitigation	Extent to which risk to the information was mitigated; distinguish verified action from assumption. §164.402(2)(iv) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>.	___ / ___

The three §164.402 exceptions are conditional: good-faith unintentional workforce/authority access within scope with no further impermissible use/disclosure; inadvertent disclosure between authorized persons within the same regulated entity or specified organized arrangement with no further impermissible use/disclosure; and good-faith belief the unauthorized recipient could not reasonably retain the information. Have counsel assess every condition; “internal,” “accidental,” or “deleted later” alone does not establish an exception. §164.402, breach definition (1)(i)–(iii) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>.

Encryption is not a blanket answer. "Unsecured" depends on HHS-specified methodology. Review what was protected, the actual implementation, and whether the confidential process/key enabling decryption was breached. A vendor badge, HTTPS alone, or an encrypted database does not establish the status of every exposed copy. Do not destroy evidence to attempt to invoke the guidance's destruction methodology. §164.402, unsecured PHI <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>; HHS secured-data guidance <https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html>.

Discovery and attribution: identify the right clock

HIPAA covered entity: discovery is the first day the breach is known or would have been known through reasonable diligence. Knowledge is attributed through workforce members or agents, excluding the person committing the breach; agent status follows federal common-law agency. **Business associate:** the parallel rule refers to employees, officers, or other agents, with the same perpetrator exclusion and federal agency standard. Counsel should evaluate whether a BA is also the covered entity's agent; separate organizations do not necessarily provide a fresh clock after leadership confirmation. §164.404(a)(2), §164.410(a)(2) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>.

FTC HBNR: discovery is when the relevant vendor, PHR-related entity, or third-party service provider knows or reasonably should know; knowledge includes employees, officers, or other agents, except the person committing the breach. Apply this rule separately rather than copying a HIPAA assessment conclusion. §318.3(c) <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318>.

HIPAA notification quick reference

Applies following discovery of a breach of unsecured PHI where the duty applies. "Without unreasonable delay" is not permission to wait until day 60. Prescribed law-enforcement delay is addressed below. §§164.404–.412 <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>.

Recipient / threshold	Timing	Official provision
Individuals whose unsecured PHI was or reasonably is believed accessed/acquired/used/disclosed	Without unreasonable delay; no later than **60 calendar days after discovery**.	§164.404(a)–(b) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>
HHS: **500 or more individuals**, not a state-residency threshold	**Contemporaneous with individual notice**; therefore subject to its without-unreasonable-delay / 60-calendar-day outside limit.	§164.408(b); §164.404(b) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>
HHS: **fewer than 500 individuals**	Maintain log/other documentation; notify HHS no later than **60 days after calendar-year end** for breaches discovered during the preceding year. Individual notice is not deferred by this annual route.	§164.408(c); §164.404(b) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>
Prominent media serving a state/jurisdiction: **more than 500 residents** of that state/jurisdiction	Without unreasonable delay; no later than **60 calendar days after discovery**. Exactly 500 does not meet this particular media threshold.	§164.406(a)–(b) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>

Recipient / threshold	Timing	Official provision
BA to covered entity	Without unreasonable delay; no later than **60 calendar days after BA discovery**; assess contractual reporting separately.	§164.410(a)–(c) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>

FTC HBNR: separate applicability and timing

Part 318 covers specified PHR vendors, PHR-related entities, and third-party providers maintaining information of US citizens/residents; it excludes HIPAA-covered entities and other entities to the extent of their business-associate activities. Apply the definitions together, including a PHR's technical capacity to draw from multiple sources. Its breach definition concerns unauthorized acquisition, including unauthorized disclosure; unauthorized access presumptively includes acquisition unless rebutted with reliable evidence. HIPAA's low-probability four-factor route is not the FTC test. §318.1–.2 <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318>.

Recipient / threshold	Current amended timing	Official provision
Required individual notice by PHR vendor/related entity	Without unreasonable delay; no later than **60 calendar days after discovery**.	§318.3(a)(1); §318.4(a) <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318>
FTC: **500 or more individuals**, not state-residency count	**Contemporaneous with individual notice** under §318.4(a), not an obsolete ten-business-day deadline.	§318.4(b); §318.5(c) <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318>
FTC: **fewer than 500 individuals**	May log and submit annually, no later than **60 calendar days after calendar-year end**, documenting preceding-year breaches; individual notice still follows its own clock.	§318.4(b); §318.5(c) <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318>
Prominent media serving state/jurisdiction: **500 or more residents** whose unsecured information is or reasonably is believed acquired	Without unreasonable delay; no later than **60 calendar days after discovery**. Unlike HIPAA media, exactly 500 meets this threshold.	§318.3(a)(3); §318.4(a) <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318>
Third-party provider to designated vendor/entity official, or senior official if none designated	Without unreasonable delay; no later than **60 calendar days after discovery**; obtain acknowledgment of receipt.	§318.3(b); §318.4(a) <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318>

Delay and notice-content guardrails

Law enforcement: HIPAA §164.412 requires delay for a qualifying official statement that notice would impede a criminal investigation or damage national security: written statement specifies the period; an oral statement must be documented, including official identity, and supports no more than 30 days unless a qualifying written statement arrives during that period. This is not discretionary delay for reputational concerns. FTC §318.4(d) separately requires delay on the specified law-enforcement determination and incorporates the implementation approach in §164.528(a)(2), including written-period/oral-documentation limits. Have counsel verify the authority and record the basis

securely. §164.412 <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>; §318.4(d) <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318>; §164.528(a)(2) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.528>.

Non-exhaustive content reminder: HIPAA individual notices require plain language and, to the extent possible, event/discovery dates if known, data types, protective steps, response, and contact procedures. Apply the actual method/substitute-notice provisions. FTC §318.6 adds known acquiring-third-party identity, with a description permitted when full identity poses the stated risk, and contact procedures using at least two specified channels: toll-free phone, email, website, within-application, or postal address. Both summaries require full-rule review; do not build a live notice solely from this sheet. §164.404(c)–(d) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>; §318.5–.6 <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318>.

Deadline register — references only

Duty / recipient role	Governing provision or contract	Discovery/trigger candidate and zone	Confirmed deadline / reviewer role	Restricted evidence reference / status
—	—	—	—	—
—	—	—	—	—
—	—	—	—	—

Keep the sensitive chronology elsewhere. Revisit uncertain counts, residency, discovery/agency, notice methods, secured status, contractual duties, and state law with counsel without stalling live response. No numerical score, fine, probability, launch approval, or privilege conclusion follows from this register.

Official sources and internal editorial notes

All opened November 7, 2026 (PST): current eCFR HIPAA Subpart D; current FTC Part 318; HHS secured-data guidance; HHS-hosted joint HHS/FTC guidance; and §164.528. eCFR is continuously updated and unofficial. Current rule text controls the timing tables; the joint guidance is contextual, not the source for amended deadlines.

- Legal interpretations, role/temporal applicability, discovery attribution, secured-data status, assessment, notice content/methods and other-law duties remain; qualified legal/editorial review and prepublication source recheck required.
- The standalone FTC compliance-guidance URL attempted returned 404; current Part 318 was opened in full and supports every FTC timing/content statement. No inaccessible guidance is treated as verified authority.
- No PAHL compliance, BAA, emergency-response capability, deliverable, or prevention guarantee asserted. Draft/publication hold remains.
- Markdown source with companion house draft PDF; no Page/live form, submission, upload, publication, or distribution implemented. No patient data should enter this sheet or booking.

The inactive booking CTA is for a proposed introductory discussion, **not an emergency service**. Do not wait for it to escalate or respond.

Book a free 30-minute audit