Palo Alto Health Labs

HIPAA Penalty Exposure Worksheet

Not legal advice. Not a compliance certification.

Not legal advice, a compliance determination, or a prediction of enforcement.

Opening takeaway: Record what happened, what was known, what should reasonably have been known, and what was corrected. Do not use vulnerability severity or breach size as a substitute for the statutory culpability analysis. The civil categories turn on knowledge, reasonable diligence, reasonable cause, willful neglect, and correction—not a technical severity score. [2][3][5]

Part B — Worksheet master (proposed downloadable content)

Before filling in anything

- Use this only within your organization's approved review process. Engage responsible legal, privacy, and security teams promptly.
- **Do not enter actual PHI, patient identifiers, clinical narratives, secrets, credentials, production URLs containing identifiers, or uploaded records.** Use generic data categories and sanitized internal evidence-reference codes only. Keep underlying evidence in authorized systems—not attached to this worksheet or sent to an introductory booking.
- Record role labels rather than personal contact details. Use a project alias with no patient information.
- Do not delete or alter evidence to make a problem disappear. Have authorized responders preserve it and contain ongoing exposure under the response plan.
- Do not assume this working document is legally privileged. Ask counsel how to handle it.
- Use MOCK/SYNTHETIC examples for demonstrations. Unknown facts stay unknown; distinguish verified evidence from assumptions.

Project alias: _____ App version/environment: _____ Worksheet date/time and zone: _____

Review status: [ ] Initial facts only [ ] Evidence gathering [ ] Legal review pending [ ] Other: _____

Responsible role labels: clinical _____ / security _____ / privacy _____ / legal _____

1. Applicability and role

HIPAA applies to covered entities and business associates; provider status includes specified standard electronic transactions. A health-related app or a physician's involvement alone does not decide the issue. [1]

Operator's proposed role: [ ] Covered entity [ ] Business associate [ ] Subcontractor [ ] Other [ ] Unknown / legal review needed

Whose behalf does the app serve? Describe the relationship, without patient details: _____

Information status: [ ] Entirely MOCK/SYNTHETIC [ ] Potential PHI/ePHI [ ] Other data [ ] Unknown / legal review needed

Legal reviewer rationale and evidence-reference code: _____

If HIPAA may not apply, assign a separate review of the FTC HBNR and other applicable law. The HBNR has its own scope and excludes business-associate activities to the stated extent; it is not the same test as HIPAA breach analysis. [12]

Separate-law review owner/status: _____

2. Map the flow before discussing culpability

For each row record only generic categories, service scope, and sanitized references. A vendor's role depends on the actual work and data flow; storing encrypted ePHI without a key can still create business-associate obligations. [10]

Boundary	Generic data category/purpose	Vendor role and service scope	Agreement/configuration evidence code	Unknown / reviewer
Builder/code generation	_____	_____	_____	_____
Preview/build/deployment	_____	_____	_____	_____
Production hosting	_____	_____	_____	_____
Model endpoint	_____	_____	_____	_____
Database/storage/backups	_____	_____	_____	_____
Telemetry/support/connectors	_____	_____	_____	_____

3. Incident triage — do not postpone response

A suspected security incident, an impermissible disclosure, and a reportable breach are not interchangeable conclusions. Under HIPAA, an impermissible use/disclosure is presumed a breach unless an applicable exception or a documented assessment demonstrating low probability of compromise applies. The assessment considers at least data nature/extent, recipient, actual acquisition/viewing, and mitigation. No numeric probability is requested here. [6][7]

Current status: [ ] Suspected incident [ ] Impermissible use/disclosure suspected [ ] Breach assessment underway [ ] Unknown / legal review needed

Immediate escalation role and time/zone: _____

Approved containment action / owner / evidence code: _____

Evidence preserved by authorized responder / location code: _____

Four-factor assessment owner and restricted-record reference (not its sensitive contents): _____

Conclusion: [ ] Pending [ ] Exception proposed for review [ ] Low-probability conclusion proposed with supporting assessment [ ] Required notice being prepared [ ] Unknown / legal review needed

Reviewer / rationale reference / next action: _____

An empty log or an assertion that nobody complained does not itself document the required assessment. HHS places the burden on the applicable regulated entity to demonstrate required notice or why notification was not required. [7]

4. Knowledge and response timeline

Record facts separately for each potentially violated provision. The earliest alert, actual knowledge of a violation, constructive knowledge, and breach discovery may differ; have counsel determine the legally relevant dates. [3][4][8][9]

Event	Date/time and zone, or unknown	What was known (sanitized)	Evidence code	Reviewer
Potential failure began	_____	_____	_____	_____
First warning or complaint	_____	_____	_____	_____
Actual knowledge of possible violation	_____	_____	_____	_____
When reasonable diligence might have revealed it	_____	_____	_____	_____
Potential breach discovery	_____	_____	_____	_____
Containment	_____	_____	_____	_____
Correction claimed	_____	_____	_____	_____
Correction independently checked	_____	_____	_____	_____

5. Facts relevant to the four categories—not a self-classification

Reasonable diligence means expected business care and prudence under similar circumstances. Reasonable cause includes actual or constructive knowledge of a violation without willful neglect. Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply. These are legal concepts, not synonyms for “severe vulnerability,” “large breach,” or “bad outcome.” [2]

For **every** row select: [ ] Evidence supporting possible category [ ] Evidence inconsistent [ ] Unknown / legal review needed. Do not add points or choose a final tier.

Possible civil category	Questions for fact gathering	Selection / supporting and contrary evidence codes
No knowledge despite reasonable diligence	What checks existed? What would appropriate diligence have revealed? What evidence supports both lack of knowledge and reasonable diligence?	_____
Reasonable cause, not willful neglect	What was known or reasonably knowable? What circumstances, resources, and response bear on the absence of willful neglect?	_____
Willful neglect, timely corrected	What evidence might show conscious failure/reckless indifference? What exact obligation was corrected, when, and how verified?	_____
Willful neglect, not timely corrected	What evidence bears on willful neglect and an uncorrected obligation beyond the relevant period? What timing remains disputed?	_____

The category distinctions and correction framework come from the statute and Enforcement Rule; this worksheet does not decide which applies. [3][5]

6. Correction is not universal immunity

For post-February 17, 2009 violations, §160.410(c) describes an affirmative defense when a violation is not due to willful neglect and is corrected within the specified **30-day** period from actual/constructive knowledge, or an additional period the Secretary determines appropriate. The statute contains qualifiers, correction/extension provisions, and possible reductions. Do not assume an extension exists because it was requested, or that a correction erases separate notice duties. [4][5][8][9]

Provision potentially violated: _____ Legal interpretation owner: _____

What counts as correction of this obligation? _____ / Unknown: _____

Actual/constructive knowledge date for review: _____

Correction due-date analysis / authority / assumptions: _____

Extension: [ ] Not assessed [ ] Requested, not established [ ] Determined by Secretary (reference) [ ] Unknown / legal review needed

Correction completed / verification evidence / remaining gaps: _____

7. Deadline register — no universal countdown

Individual HIPAA breach notices and BA notices have “without unreasonable delay” requirements and outside **60-calendar-day** limits after applicable discovery, subject to the cited law-enforcement exception. Contracts can require earlier BA reporting; other notice recipients and laws have different rules. Do not wait for the outside limit or start every clock at worksheet completion. [8][9][10]

Possible duty	Governing rule/contract and triggering facts	Discovery/trigger date	Deadline confirmed by reviewer	Owner / action / status
Incident escalation/contract report	_____	_____	_____	_____
BA-to-customer notification	_____	_____	_____	_____
Individual notification	_____	_____	_____	_____
HHS/media/other regulator review	_____	_____	_____	_____
FTC/state/other-law review	_____	_____	_____	_____
Correction / any approved extension	_____	_____	_____	_____

8. Legal review handoff

Questions still unresolved: _____

Next action / role owner / due date: _____

Legal assessment status: [ ] Not started [ ] Pending more facts [ ] Reviewed with limitations [ ] Unknown

Assessment reference and scope limitations: _____

Stop here. No dollar output, probability, self-certified tier, or compliance pass/fail follows from completing this document. Keep response work moving while questions are reviewed.

Primary sources

All accessed November 7, 2026 (PT). Bracketed source IDs are stable within this worksheet/scenario set.

- [1] HHS: Covered Entities and Business Associates <https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html>.
- [2] 45 CFR 160.401: culpability definitions <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-160/subpart-D/section-160.401>.
- [3] 45 CFR 160.404: civil penalty categories <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-160/subpart-D/section-160.404>.
- [4] 45 CFR 160.410: affirmative defenses <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-160/subpart-D/section-160.410>.
- [5] 42 USC 1320d–5: statutory penalties, limitations, extensions <https://uscode.house.gov/us/usc/119-136/t42/s1320d-5/>.
- [6] 45 CFR 164.402: breach definition and assessment <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D/section-164.402>.
- [7] HHS: Breach Notification Rule guidance <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>.

- [8] 45 CFR 164.404: individual notice and discovery <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D/section-164.404>.
- [9] 45 CFR 164.410: business associate notification <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D/section-164.410>.
- [10] HHS: HIPAA & Cloud Computing <https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html>.
- [12] 16 CFR Part 318: FTC Health Breach Notification Rule <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318>.

Limits

No PAHL compliance, BAA, capability, or prevention guarantee.