Palo Alto Health Labs

# The Practice Tech Audit — Fractional CTO Self-Assessment

**Not legal advice. Not a compliance certification.**

A dedicated fractional CTO topic worksheet for practice technology decisions—not a proposal to change sitewide positioning. Use it to identify ownership gaps and questions for a technical discussion. It does not represent a PAHL assessment, an engagement deliverable or a certification.

Practice/project label: _____ Review date: _____
Business decision owner: _____ Technical contact: _____
Clinical workflow owner: _____ Security/legal contact: _____
Top workflow frustration: _____
Decision needed and target date: _____

## How to use this self-assessment

Choose Known / Open / Not applicable for each prompt. Attach only approved evidence references; explain Not applicable. Do not calculate a numerical maturity/compliance score. A known issue may be urgent even when every other response is Known.

## A. Workflow and portfolio

- Which tools are essential for daily operation? _____
- Which workflows depend on one person's knowledge? _____
- Which duplicated entries or manual handoffs deserve investigation? _____
- Which proposed tools have an agreed user, purpose and excluded uses? ____

Status / evidence / accountable owner: _____

## B. Vendors, contracts and access

- Is there an inventory of exact products, accounts and owners? _____
- Who approves vendors and feature changes? _____
- Where required, who verifies signed BAAs and eligible services? _____
- Who grants/removes staff and administrator access? _____
- How are privileged authentication and credential rotation reviewed? ____
- Where do support, model, analytics and backup copies go? _____

Status / evidence / accountable owner: _____

## C. Reliability and recovery

- Who notices a failure and who can act? _____
- When was restoration last rehearsed, and what evidence exists? _____
- What work continues during downtime and how is it reconciled? _____
- Who owns patching, dependencies and configuration changes? _____
- Is there a reversible change/cutover process? _____

Status / evidence / accountable owner: _____

## D. EHR and data boundaries

- Which system is authoritative for each record/work item? _____
- Who approves API permissions and organization-specific testing? _____
- Can the team explain patient/encounter matching and context changes? ____
- Which read-only or write-back operations are enabled? _____
- How are partial results, denied access and stale data shown? _____

FHIR is not itself a security protocol, and an API connection is not a compliance certificate. Implementers must address access control and other safeguards.

Status / evidence / accountable owner: _____

## E. AI and physician-built tools

- Which tools receive prompts, uploads or generated outputs? _____
- Are coding tools separated from approved production data processing? ___
- Who approves intended use and reviews clinical output where relevant? __
- Are generated drafts distinguished from accepted records/actions? _____
- Is keep/refactor/rebuild a documented component decision? _____

These are proposed review prompts, not clinical validation criteria.

Status / evidence / accountable owner: _____

## F. Convert uncertainty into an owned decision

| Issue | Evidence or impact to investigate | Interim action | Owner | Due / review trigger |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

Choose next path: Internal clarification / Vendor documentation review / Technical assessment discussion / Pause a proposed change.

Reason: _____
Questions to bring to a consultation, without sensitive records:
1. _____
2. _____
3. _____

HHS's cloud guidance pairs BAAs with risk analysis, safeguards and shared responsibilities. Completing this self-assessment establishes none of those by itself.

## 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.
- HL7 FHIR R4 security <https://hl7.org/fhir/R4/security.html>, opened/read 2026-11-07 PST.
- This resource contains proposed management prompts, not data about practice performance or PAHL client outcomes.


## 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.