Palo Alto Health Labs

Practice Technology Roadmap Template (12 months)

Not legal advice. Not a compliance certification.

Not legal advice, not a completed security or HIPAA assessment, and not a finding of compliance.

Document type: Downloadable / printable worksheet. Fill in the blanks. Do not paste real patient names, record numbers, or other patient information into this form.

Proposed public title: Practice Technology Roadmap Template (12 months)

How to use this: Complete it with your administrator, any in-house IT staff or managed service provider (MSP), and the people who actually run the EHR, billing, and front desk. Review it with qualified privacy counsel before you treat any legal conclusion as settled. Update it when systems, locations, or unofficial tools change.

What this is not: Completing this template does not, by itself, satisfy the HIPAA Security Rule, complete a risk analysis, or certify any vendor or tool. HHS does not endorse, certify, or recommend specific technology or products (HHS cloud-computing guidance, question 4 <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html>, accessed November 7, 2026, PT).

Official sources cited below were opened on Saturday, November 7, 2026, America/Los_Angeles (Pacific Time).

Document control

Field	Entry
Practice name	_____
Locations covered	_____
Roadmap period	From _____ to _____ (12 months)
Version / date	_____
Prepared by	_____
Approved by (practice owner / managing partner)	_____
Next scheduled review	_____
Security official (if designated)	_____
Privacy official (if designated)	_____
IT operations contact (in-house or MSP)	_____

Field	Entry
Counsel / privacy advisor (if any)	_____

HHS's Security Rule summary states that a regulated entity must designate a security official responsible for developing and implementing the policies and procedures required by the Security Rule (HHS Security Rule summary <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>, accessed November 7, 2026, PT). Whether your organization is a regulated entity is fact-specific.

1. Practice goals for the next 12 months

Write outcomes the practice actually wants, not a list of products. Examples of outcome language (replace with your own): reduce duplicate data entry between two named systems; prepare a second location to use the same core systems; decide whether a physician-built tool may move beyond prototype; complete a documented vendor comparison before a contract renewal.

#	12-month goal	Why it matters now	Owner	Target date	How we will know it worked	Status (not started / in progress / done / paused)
1						
2						
3						
4						
5						

Constraints to keep in view (staffing, lease, planned leaves, known contract end dates — no patient data):

\1

\1

2. Baseline inventory

List what the practice actually uses, including unofficial spreadsheets, shared inboxes, and tools individual clinicians built. HHS risk-analysis guidance says an organization must identify where ePHI is stored, received, maintained, or transmitted, and that the analysis should take into account all of its ePHI regardless of medium, source, or location (HHS Guidance on Risk Analysis <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>, accessed November 7, 2026, PT). This inventory is a worksheet to support that work. It is not the risk analysis itself.

ONC, in collaboration with OCR, provides a Security Risk Assessment Tool intended to help small and medium providers walk through an assessment. ONC states that use of the tool is neither required by nor a guarantee of compliance (ONC Security Risk Assessment Tool <https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool>, accessed November 7, 2026, PT).

Do not write sample patient records here. Describe categories (for example: “appointment demographics,” “claim files,” “none identified”) rather than examples copied from a chart.

2a. Core systems

System / product	Vendor	What it is used for	Information categories (no patient examples)	Integrates with	Administrative owner	Clinical / operational owner	Contract end or renewal date	Notes
EHR								
Practice management								
Billing / clearinghouse								
Patient communication / portal								
Phone / messaging								
Identity / email / productivity								
Backup / disaster recovery								
Other: _____								
Other: _____								

2b. Unofficial, homegrown, or physician-built tools

Tool (plain name)	Who built or introduced it	What it does	Can it see or change patient or billing information? (yes / no / unknown)	Where it runs (device, vendor, unknown)	Who holds logins and source code?	Approved for production use? (yes / no / unknown)	Action

2c. People who keep technology running

Role	Name	Organization (practice / MSP / vendor / other)	What they own day to day	How to reach them	Backup person

3. Owners and decision rights

Overlapping work is normal. An MSP or in-house technician may implement a change that an owner, administrator, or fractional technology leader decided. Write down who is accountable (has the final yes/no) and who does the work.

Decision	Accountable (final yes/no)	Responsible (does the work)	Consulted	Informed	Notes
Approve this 12-month roadmap					
Select or replace an EHR, PM, or billing system					
Approve a new vendor or AI tool					
Approve a physician-built tool for production use					
Day-to-day device, account, and ticket work					
Report and coordinate a suspected security incident					
Update the security risk analysis after new technology is planned					
Sign or renew vendor contracts and BAAs (with counsel)					
Retire or revoke access when someone leaves					

HHS's Security Rule summary states that regulated entities must implement policies and procedures to address security incidents, and must identify, respond to, mitigate, and document them (HHS Security Rule summary <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>, accessed November 7, 2026, PT).

4. Dependencies

Initiative or milestone	Depends on (system, vendor, person, contract, or decision)	What happens if this slips	Owner	Mitigation

5. Twelve-month phased milestones

Put only work the practice can staff. Leave unused rows blank. Each milestone should name an outcome, not only a meeting.

Phase 1 — Months 1 to 3

Focus for this phase: _____

Milestone	Outcome we will be able to point to	Owner	Dependencies	Security / privacy / safety checkpoint (see section 6)	Target date	Status

Phase 2 — Months 4 to 6

Focus for this phase: _____

Milestone	Outcome we will be able to point to	Owner	Dependencies	Security / privacy / safety checkpoint (see section 6)	Target date	Status

Phase 3 — Months 7 to 9

Focus for this phase: _____

Milestone	Outcome we will be able to point to	Owner	Dependencies	Security / privacy / safety checkpoint (see section 6)	Target date	Status

Phase 4 — Months 10 to 12

Focus for this phase: _____

Milestone	Outcome we will be able to point to	Owner	Dependencies	Security / privacy / safety checkpoint (see section 6)	Target date	Status

6. Security, privacy, and safety checkpoints

Use these as review gates, not as a claim that any one checkbox equals compliance. HHS says risk analysis is required for regulated entities, is not one-size-fits-all, and should be ongoing; planning to incorporate new technology is a reason to analyze risk again. HHS also says the Security Rule does not specify a single required frequency (HHS Guidance on Risk Analysis <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>, accessed November 7, 2026, PT).

HHS notes that some of its risk-analysis discussion draws on NIST guidance, and that only federal agencies are required to follow NIST guidelines, though non-federal organizations may find them useful (HHS Guidance on Risk Analysis <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>, accessed November 7, 2026, PT). NIST SP 800-66 Revision 2 is a cybersecurity resource guide for implementing the HIPAA Security Rule, published February 2024 (NIST SP 800-66r2 <https://csrc.nist.gov/pubs/sp/800/66/r2/final>, accessed November 7, 2026, PT).

CISA's Cross-Sector Cybersecurity Performance Goals 2.0 are described by CISA as voluntary practices intended to help small- and medium-sized organizations prioritize high-impact actions; CISA notes updates that address, among other topics, risks associated with managed service providers (CISA Cross-Sector CPGs <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>, accessed November 7, 2026, PT). HHS has also published voluntary Healthcare and Public Health Cybersecurity Performance Goals, built on CISA's CPG chassis (HHS HPH CPGs <https://hhscyber.hhs.gov/cybersecurity-performance-goals.html>, accessed November 7, 2026, PT; also noted on CISA's healthcare cybersecurity page <https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare>, accessed November 7, 2026, PT). These are not presented here as HIPAA mandates.

Clinical safety (what a tool does to care) is a separate review from privacy and security (where information goes and who can see it).

Checkpoint	When to use it	Owner	Evidence location (policy, ticket, report — no PHI)	Date done	Result / follow-up
Inventory includes unofficial and physician-built tools	At kickoff and after any new tool appears				
Confirm, with counsel, whether the practice is a HIPAA covered entity or business associate for the activity in question	Before drawing legal conclusions from this roadmap				
Update risk analysis if new technology is planned or after a security incident, ownership change, or key-staff turnover	Before production use of a new system or custom tool				
Identify vendors that may create, receive, maintain, or transmit ePHI and record whether a BAA question has been reviewed with counsel	Before a new vendor or cloud tool handles that information				
No real patient data in unapproved prototypes or consumer AI accounts	Every prototype review				
Access is limited to people who need it; departing workforce access is revoked	At hire/leave and when a tool goes live				
Backup and recovery steps for systems that hold ePHI are written and have an owner	Before depending on a system clinically or operationally				
Suspected security-incident contacts and first steps are written down	Before an incident, then after any test or event				
If a tool can influence documentation or care, a named clinician reviews intended use, known failure modes, and rollback *before* production use	Before clinical-impacting production use				
Roadmap review after any material vendor, location, or tool change	As changes occur				

HHS's Security Rule summary describes contingency-plan expectations for regulated entities, including backing up ePHI, restoring lost data, and continuing critical processes in emergency mode (HHS Security Rule summary <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>, accessed November 7, 2026, PT).

7. Cost worksheet (blank fields only)

Do not copy vendor marketing prices into this section unless you replace them with figures from *your* quotes. Leave unused rows blank. This section records the practice's own numbers; this draft publishes no PAHL prices and no sample dollar amounts.

Initiative or contract	One-time cost	Recurring cost	Period (monthly / annual / other)	Estimated internal staff hours	Whose budget	Quote or invoice reference (no account secrets)	Notes
	$ _____	$ _____					
	$ _____	$ _____					
	$ _____	$ _____					
	$ _____	$ _____					
	$ _____	$ _____					

Total one-time (practice to calculate): $ _____

Total recurring per year (practice to calculate): $ _____

What we will *not* fund this year, and why:

\1

\1

8. Success measures

Measure (plain language)	Baseline today	Target by end of 12 months	How we will check	Owner	Result
Example to replace: “We can name an owner for every system in section 2.”					

9. Review cadence

HHS does not prescribe a single calendar interval for risk analysis; it says the process should be ongoing and should consider new technology, incidents, and other environmental changes (HHS Guidance on Risk Analysis <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>, accessed November 7, 2026, PT). Choose a cadence the practice will actually keep.

Review	Suggested purpose	Cadence we will use	Who attends	Next date
Operational check-in	Tickets, outages, access changes, unofficial tools that appeared	Weekly / biweekly / monthly: _____		
Roadmap review	Milestone status, dependencies, budget blanks, paused work	Quarterly: _____		
Security / privacy checkpoint	Risk-analysis updates, vendor/BAA questions for counsel, incident lessons	At least when new technology is planned, and also: _____		
Annual reset	Write the next 12-month roadmap	Each year in: _____		

Notes from the latest review (no patient information):

\1

\1

\1

Official sources opened November 7, 2026, PT

1. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
2. https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html
3. https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html
4. https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool
5. https://csrc.nist.gov/pubs/sp/800/66/r2/final
6. https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
7. https://hhscyber.hhs.gov/cybersecurity-performance-goals.html
8. https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare

Limits

The conversation is not a completed security assessment, not a HIPAA certification, and not a finding of compliance.

Do not send patient records, screenshots of real charts, or credentials when requesting a conversation.

Fillable worksheet; no PAHL pricing figures; no sample dollar amounts.