Palo Alto Health Labs

EHR / vendor contract review checklist

Not legal advice. Not a compliance certification.

Document type: Downloadable / printable review aid for a named vendor contract, order form, statement of work, service-level exhibit, or business associate agreement.

This is not legal advice and not a model contract. Completing it does not create, replace, or negotiate an agreement. It does not determine whether HIPAA applies to your organization or to a particular vendor. Take unanswered legal questions to qualified counsel. Do not paste patient information, credentials, or full contract secrets into this form; quote clause titles or section numbers instead.

How to use the "Type" column

- **Question** — something the practice should be able to answer from the documents or from the vendor, so owners know what they are buying.
- **Requirement pointer** — a short note about what an official HHS, ONC, CISA, or NIST source says, so you can compare the documents with published guidance. A pointer is not a finding that the cited rule applies to your facts.

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

Review header

Field	Entry
Practice name	_____
Vendor / product being reviewed	_____
Agreement titles and dates in the packet	_____
Review date	_____
Reviewer	_____
Counsel reviewing legal questions (if any)	_____
Intended go-live or renewal date	_____
Recommendation (proceed / proceed with changes / do not proceed / needs counsel)	_____

Related practice owner for this vendor: _____

1. Service scope

#	Type	Review item	What we found / evidence (section or exhibit)	Owner	Action	Status
1.1	Question	What services, modules, environments, and locations are included?				
1.2	Question	What is expressly out of scope (interfaces, data conversion, training, after-hours support, custom work)?				
1.3	Question	Which party provides implementation, configuration, and ongoing administration?				
1.4	Question	Can the vendor change the service materially (features, hosting region, subprocessors) without the practice's written consent?				
1.5	Question	Is professional-services work (migration, interface build, optimization) described with deliverables, or only as hourly assistance?				

2. Roles and responsibilities

#	Type	Review item	What we found / evidence	Owner	Action	Status
2.1	Question	Who is the practice's named relationship owner, and who is the vendor's named counterpart?				
2.2	Question	What does the practice still have to do (workstation standards, user provisioning, downtime procedures, end-user training)?				
2.3	Question	If an MSP or in-house IT team will support devices that reach this system, is that division of labor written down?				
2.4	Requirement pointer	HHS lists an IT contractor or vendor — and gives "EHR vendor, Managed Services Provider" as examples — among persons who may be business associates when they provide maintenance or support that requires them to create, receive, maintain, or transmit ePHI (HHS business associate FAQs <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html>, accessed November 7, 2026, PT). This is an example list, not an automatic label for every IT company. Ask counsel whether *this* vendor's actual work creates that relationship.				

3. Business associate agreement applicability

Do not treat a marketing page that says “HIPAA compliant” as a substitute for executed terms. HHS states that OCR 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).

#	Type	Review item	What we found / evidence	Owner	Action	Status
3.1	Question	Will this vendor create, receive, maintain, or transmit protected health information for the practice?				
3.2	Question	Is a BAA already executed for the exact legal entity and the exact service being purchased?				
3.3	Requirement pointer	If a covered entity engages a business associate, HHS says the covered entity must have a written business associate contract or other arrangement that says what the associate has been engaged to do and requires it to protect PHI (HHS: Covered Entities and Business Associates <https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html>, accessed November 7, 2026, PT).				
3.4	Requirement pointer	HHS says a cloud service provider engaged to create, receive, maintain, or transmit ePHI on a regulated entity’s behalf is a business associate even if it stores only encrypted ePHI and lacks the encryption key. Using such a CSP without a BAA is described as a HIPAA Rules violation (HHS cloud-computing guidance <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html>, accessed November 7, 2026, PT).				
3.5	Requirement pointer	HHS describes the conduit exception as limited to transmission-only services, including temporary storage incident to transmission. Entities with more persistent access, including CSPs that store ePHI, generally are not conduits (HHS cloud-computing guidance, question 3 <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html>; HHS business associate FAQs <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html>, accessed November 7, 2026, PT).				
3.6	Question	Do the BAA’s permitted uses and disclosures match how the product actually works (support access, analytics, model training, overseas support)?				
3.7	Requirement pointer	HHS summarizes required BAA content, including permitted uses/disclosures and limits on further use, and points to sample BAA provisions (HHS business associate FAQs <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html>; HHS sample BAA provisions <https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>, accessed November 7, 2026, PT). Compare your draft to counsel’s reading of those elements; do not treat the sample as your contract.				

4. Subprocessors and downstream parties

#	Type	Review item	What we found / evidence	Owner	Action	Status
4.1	Question	Has the vendor named the subprocessors, hosting providers, AI model providers, support tools, and analytics vendors that may receive practice data?				
4.2	Question	How is the practice notified if that list changes?				
4.3	Requirement pointer	HHS says a business associate must establish a BAA with its subcontractor before disclosing PHI to that subcontractor for work done for a covered entity, and that downstream subcontractors are also business associates (HHS business associate FAQs <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html>, accessed November 7, 2026, PT).				
4.4	Requirement pointer	The Security Rule, as summarized by HHS, requires BAAs to commit the business associate to ensuring that subcontractors that handle ePHI agree to comply with the Security Rule through their own BAA (HHS Security Rule summary <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>, accessed November 7, 2026, PT).				

5. Data use, retention, and AI training

#	Type	Review item	What we found / evidence	Owner	Action	Status
5.1	Question	For what purposes may the vendor use practice or patient information (providing the service, improving the product, advertising, training models)?				
5.2	Question	Is use of identifiable, de-identified, or aggregated data for model training allowed, prohibited, or silent?				
5.3	Question	Where is data stored or accessed (regions, remote support, offshore personnel)?				
5.4	Requirement pointer	HHS states that HIPAA Rules do not forbid using a CSP that stores ePHI on servers outside the United States if a BAA is in place and other applicable requirements are met, but notes that location can change risk and should be considered in risk analysis (HHS cloud-computing guidance, question 9 <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html>, accessed November 7, 2026, PT).				
5.5	Question	How long is data retained after the service ends, and who decides?				

#	Type	Review item	What we found / evidence	Owner	Action	Status
5.6	Requirement pointer	HHS says a CSP that receives and maintains only information de-identified in accordance with the Privacy Rule is not a business associate for that information (HHS cloud-computing guidance, question 11 <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html>, accessed November 7, 2026, PT). "De-identified" here means HHS's process, not informal removal of a name.				

6. Access, export, and portability

#	Type	Review item	What we found / evidence	Owner	Action	Status
6.1	Question	Can the practice access, export, and produce its data in a usable format during the term and at exit? In what formats, at what frequency, and at what extra fee (record the fee from *your* quote only)?				
6.2	Question	What happens if the vendor suspends the account for a billing or dispute reason — can the practice still reach records needed for care?				
6.3	Requirement pointer	HHS cautions that SLA and BAA terms should not prevent a regulated entity from accessing its ePHI, and points to the prohibition on a business associate blocking or terminating customer access inconsistently with the Rules (HHS cloud-computing guidance, question 1 and note 11 <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html>, accessed November 7, 2026, PT).				
6.4	Requirement pointer	ONC states that information blocking is a practice by an "actor" likely to interfere with access, exchange, or use of electronic health information, except as required by law or covered by an exception, and that the Cures Act applied the law to healthcare providers, health IT developers of certified health IT, and HIEs/HINs. Knowledge standards differ by actor type (ONC: Information Blocking <https://www.healthit.gov/topic/information-blocking>, accessed November 7, 2026, PT). Whether a contract term or a practice creates an information-blocking issue is a case-specific legal question for counsel, not something this checklist decides.				

7. Integration responsibilities

#	Type	Review item	What we found / evidence	Owner	Action	Status
7.1	Question	Which interfaces are included (EHR, PM, lab, imaging, clearinghouse, patient app), and which are extra projects?				
7.2	Question	Who writes, tests, monitors, and repairs each interface? What is the expected turnaround when an interface fails?				
7.3	Question	Who pays if the other system changes its API or interface specification?				
7.4	Question	Are there volume, transaction, or message caps that would affect a growing practice?				

8. Security evidence

HHS's Healthcare and Public Health Cybersecurity Performance Goals include a *voluntary* essential goal on vendor/supplier cybersecurity requirements: identify, assess, and mitigate risks associated with third-party products and services (HHS HPH CPGs <https://hhscyber.hhs.gov/cybersecurity-performance-goals.html>, accessed November 7, 2026, PT). CISA describes its Cross-Sector CPGs as voluntary baseline practices (CISA Cross-Sector CPGs <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>, accessed November 7, 2026, PT).

#	Type	Review item	What we found / evidence	Owner	Action	Status
8.1	Question	What written security practices, certifications, pen-test summaries, or questionnaires did we actually receive?				
8.2	Requirement pointer	HHS states that the HIPAA Rules do *not* expressly require a CSP to give customers documentation of its security practices or to allow customer audits. Customers may still require additional assurances through the BAA, an SLA, or other documents, based on their own risk analysis (HHS cloud-computing guidance, question 10 <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html>, accessed November 7, 2026, PT). Asking for evidence is a practice decision; it is not written here as a universal statutory mandate.				
8.3	Question	How is privileged vendor access to the practice's environment granted, logged, and revoked?				
8.4	Question	Does the packet describe encryption in transit and at rest, unique user identification, and audit controls — and who is responsible for turning them on?				

#	Type	Review item	What we found / evidence	Owner	Action	Status
8.5	Requirement pointer	The Security Rule, as summarized by HHS, requires regulated entities to implement reasonable and appropriate administrative, physical, and technical safeguards, including access control, audit controls, integrity protections, authentication, and transmission security, with flexibility based on size, complexity, capabilities, costs, and risk (HHS Security Rule summary <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>, accessed November 7, 2026, PT). Mapping those topics in a contract review is not the same as completing the practice's own risk analysis.				

9. Incident notification

#	Type	Review item	What we found / evidence	Owner	Action	Status
9.1	Question	How quickly must the vendor notify the practice of a security incident or a suspected breach, and through what channel?				
9.2	Question	What facts will the notice include (systems affected, data categories, timeframe, mitigation)?				
9.3	Requirement pointer	HHS says a business associate CSP must implement policies to address and document security incidents and must report security incidents of which it becomes aware. The Security Rule does not prescribe one format or frequency for ordinary security-incident reports, which parties may work out in the BAA (HHS cloud-computing guidance, question 6 <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html>, accessed November 7, 2026, PT).				
9.4	Requirement pointer	If a breach of unsecured PHI occurs at or by a business associate, HHS says the business associate must notify the covered entity without unreasonable delay and no later than 60 days from discovery, and should identify affected individuals to the extent possible (HHS Breach Notification Rule <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>, accessed November 7, 2026, PT). A contract may be more protective than this outer timeline; it should not undercut applicable notice duties. Whether an event is a "breach" is a legal determination.				
9.5	Question	Who pays for investigation, notification, and mitigation assistance if the vendor's environment is involved? (Record terms from *this* packet only; do not invent figures.)				

10. Availability, backup, and recovery

HHS notes that service-level agreements commonly address expectations that may also be relevant to HIPAA compliance, and gives examples: system availability and reliability; backup and data recovery (including ransomware or other emergencies); how data will be returned after service termination; security responsibility; and use, retention, and disclosure limitations. HHS says any SLA should be consistent with the BAA and the HIPAA Rules (HHS cloud-computing guidance, question 1 <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html>, accessed November 7, 2026, PT). These are review topics HHS lists, not a mandatory SLA outline.

#	Type	Review item	What we found / evidence	Owner	Action	Status
10.1	Question	What availability commitment is stated, how is it measured, and what happens if it is missed?				
10.2	Question	Who backs up the data, how often, where are copies stored, and who has tested a restore?				
10.3	Question	What is the documented recovery objective the vendor is willing to state, and what must the practice do during downtime?				
10.4	Requirement pointer	HHS's Security Rule summary describes contingency-plan expectations for regulated entities, including backing up ePHI, restoring lost data, and emergency-mode operation (HHS Security Rule summary <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>, accessed November 7, 2026, PT). The practice's own plan is separate from the vendor's marketing uptime number.				

11. Renewals, termination, and exit

#	Type	Review item	What we found / evidence	Owner	Action	Status
11.1	Question	What is the initial term, renewal mechanism (auto-renew or written), and notice period?				
11.2	Question	For what causes may either party terminate, and what cure period applies?				
11.3	Question	At exit, in what format, on what timeline, and at what stated fee (from this packet only) does the practice receive its data?				
11.4	Question	After export, how does the vendor delete or retain copies, including backups?				

#	Type	Review item	What we found / evidence	Owner	Action	Status
11.5	Requirement pointer	HHS says the HIPAA Rules generally do not require a business associate to keep ePHI after services end, and that a BAA must require the associate to return or destroy PHI at termination where feasible; if return or destruction is not feasible, protections continue and further uses are limited (HHS cloud-computing guidance, question 8 <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html>, citing 45 CFR § 164.504(e)(2)(ii)(J); accessed November 7, 2026, PT).				
11.6	Question	Will interfaces, custom work, and documentation created for the practice transfer, or do they remain the vendor's property?				
11.7	Question	Is there a transition-assistance period, and who staffs it?				

Reviewer conclusion (not a legal opinion)

Outstanding questions for counsel:

1. _____
2. _____
3. _____

Changes we will request before signing or renewing:

1. _____
2. _____
3. _____

Practice decision and date: _____

Official sources opened November 7, 2026, PT

1. https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html
2. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html
3. https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html
4. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

5. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
6. https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html
7. https://www.healthit.gov/topic/information-blocking
8. https://hhscyber.hhs.gov/cybersecurity-performance-goals.html
9. https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
10. https://csrc.nist.gov/pubs/sp/800/66/r2/final

NIST SP 800-66 Revision 2 is cited as a resource guide, not as a binding requirement for non-federal practices. HHS states that only federal agencies are required to follow NIST guidelines (HHS Guidance on Risk Analysis <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>, accessed November 7, 2026, PT).

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, credentials, or full contracts containing secrets when requesting a conversation.

No PAHL pricing figures.