Palo Alto Health Labs

OCR data request readiness kit

Not legal advice. Not a compliance certification.

Not legal advice, certification, or launch clearance.

Read before using

This is a non-exhaustive preparation aid. Applicability depends on the entity's role, activity, relevant period, facts, and actual request. The Security Rule applies to covered entities and business associates with respect to covered-entity ePHI; the Privacy administrative provisions below primarily address covered entities, with applicable exceptions. Do not apply every row identically to every vendor or practice. §164.302 <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>; §164.530, including (k) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.530>.

The real OCR letter, applicable law, and counsel's review determine responsive production, scope, deadlines, and extension requests; an extension is not assumed granted. Covered entities and business associates must provide records/reports as the Secretary determines necessary, cooperate, and permit pertinent access under §160.310. This kit supplies no universal OCR response deadline or substitute request list. §160.310(a)–(c) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-160/subpart-C/section-160.310>.

Urgent suspected incidents: promptly contact responsible incident responders and privacy/security leadership; involve counsel as appropriate. Do not wait for this worksheet or a booking. The Security Rule requires response to suspected or known incidents and documentation of incidents/outcomes. §164.308(a)(6)(ii) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.

Legend and safe completion

- **D — explicit documentation:** the cited provision expressly requires a writing, documented activity/designation, or retained documentation. Scope and conditions still matter.
- **E — suggested evidence:** useful artifacts showing operation of a required control/process; the regulation does not necessarily mandate that named artifact or format.
- **C — conditional:** depends on role, events, relationship, or an addressable assessment. C can accompany D or E; it never means disregard the requirement.

For each row record status **located / needs review / unknown / not applicable**, a generic owner role, and a neutral evidence-reference code. Record the rationale for not applicable in a separate internal note. Do not enter names, identifiers, PHI, secrets, production logs, screenshots, or underlying records. Keep real evidence in authorized restricted systems and produce only through verified, approved response channels. A reference such as `POL-01` is sufficient here; do not expose a credential-bearing link.

A policy's existence is not evidence that it operated. Locate both the applicable historical policy and operational support where relevant. Missing records must remain identified as missing: never backdate, alter originals, or fabricate prior implementation. Label newly created remediation accurately. This kit does not determine or promise privilege; counsel assesses handling questions.

Printable evidence-location checklist

Every legal summary below remains. Each row includes an adjacent requirement citation; E artifacts are recommendations, not newly named legal documents.

# / Topic	Requirement and distinction	Locate in restricted systems; enter references only	Status / owner role / reference
1. Risk analysis	**E:** accurate, thorough risk/vulnerability assessment is required; the proposed artifact names are not prescribed. §164.308(a)(1)(ii)(A) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.	Assessment versions, scope/method, findings; optional system inventory or data-flow diagram supporting coverage, including prompts, previews, logs and vendors. No mandated annual certificate.	___ / ___ / ___
2. Risk management	**E:** implement measures reducing risks/vulnerabilities to a reasonable and appropriate level. §164.308(a)(1)(ii)(B) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.	Remediation/action register, responsible roles, implementation and verification evidence; distinguish planned from completed work.	___ / ___ / ___
3. Security policies and documentation	**D:** maintain implemented policies/procedures in writing and written records of actions/assessments the subpart requires to be documented; make available and update as required. §164.316(a), (b)(1), (b)(2)(ii)–(iii) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.316>.	Historical/current policy versions, effective dates, revision records, required documented assessments; separate operation evidence from policy approval.	___ / ___ / ___
4. Assigned roles	**E:** identify security official. **D/C:** covered entity documents privacy official and complaint-contact designations. §164.308(a)(2) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>; §164.530(a)(1)–(2) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.530>.	Security responsibility record (suggested format); documented privacy/contact designations where applicable; role transitions. Do not put personal details here.	___ / ___ / ___
5. Training	**E:** security awareness/training program for workforce. **D/C:** covered entity must document specified Privacy/Breach training provided. §164.308(a)(5)(i) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>; §164.530(b)(1)–(2) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.530>.	Materials and evidence of delivery; role-appropriate content and new-worker/material-change training records. Do not infer training happened from slides alone.	___ / ___ / ___
6. Workforce and access changes	**D/E/C:** workforce security/access-management policies; addressable termination and access-establishment/modification specifications. The latter expressly includes documenting access rights. §164.308(a)(3), (a)(4)(ii)(C) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.	Authorization records, access review and joiner/mover/leaver evidence; addressable decisions and applicable documented rights. A named access spreadsheet is not universally mandated.	___ / ___ / ___
7. Authentication and technical access	**E:** technical access controls, required unique identification/emergency access, and authentication. §164.312(a), (d) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.	Configuration history, role/service-identity ownership and MOCK/SYNTHETIC authorization-test references; emergency-access procedure. No blanket MFA or RLS mandate asserted.	___ / ___ / ___
8. Activity review and audit controls	**E:** regularly review system-activity records and implement mechanisms recording/examining system activity. §164.308(a)(1)(ii)(D); §164.312(b) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.	Review procedure plus dated review/action evidence and logging configuration; restricted source-log references only, never raw logs here. Policy alone does not show review occurred.	___ / ___ / ___
9. Security incidents	**D:** identify/respond, mitigate known harmful effects as practicable, and document incidents/outcomes. §164.308(a)(6)(ii) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.	Incident procedure, discovery/response chronology, outcome and mitigation records; preserve original evidence under authorized response procedures.	___ / ___ / ___

# / Topic	Requirement and distinction	Locate in restricted systems; enter references only	Status / owner role / reference
10. Breach assessment and notification	**D/C:** applicable entity bears proof that required notices were made or the impermissible use/disclosure was not a breach; covered-entity documentation includes that proof. §164.414(b) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D/section-164.414>; §164.530(j)(1)(iv) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.530>.	Counsel-reviewed assessment/exception basis or notice records with delivery/reporting evidence as applicable; no assumption every incident is a reportable breach. HHS breach guidance <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>.	___ / ___ / ___
11. Business associates	**D/C:** document satisfactory assurances through required contract/other arrangement; role and subcontractor chain matter. §164.308(b)(1)–(3), §164.314(a) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>; §164.504(e)(1)–(3), (5) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.504>.	Applicable accepted BA agreements/arrangements and service scope. Suggested inventory helps locate them but is not itself a universally named required document; check exclusions and acceptance evidence.	___ / ___ / ___
12. Contingency operations	**E/C:** required backup, disaster-recovery and emergency-mode plans/procedures; periodic testing/revision and criticality analysis are addressable. §164.308(a)(7)(ii)(A)–(E) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.	Plans plus evidence of backup/recovery operation; suggested restore-exercise records and dependency/fallback review. Plan existence alone does not prove recovery works.	___ / ___ / ___
13. Evaluation	**E:** periodic technical/nontechnical evaluation and evaluation responding to environmental/operational changes. §164.308(a)(8) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.	Evaluation scope/results and change-trigger reviews. No blanket annual assessment frequency or annual penetration certificate is established here.	___ / ___ / ___
14. Physical/device safeguards	**D/E/C:** facility/workstation/device-media policies; addressable maintenance and movement records, and required disposal/reuse procedures. §164.310(a)–(d), especially (a)(2)(iv), (d)(2)(i)–(iii) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>; §164.316(b)(1) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.316>.	Applicable written procedures, device/media movement and maintenance evidence under assessed specifications, restricted disposition records and safeguard checks. Do not destroy evidence to complete this row.	___ / ___ / ___
15. Privacy policies, complaints and sanctions	**D/C:** covered entity maintains written policies, documents complaints/dispositions and sanctions applied, subject to applicable exceptions. §164.530(d)(2), (e), (i), (j) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.530>.	Policy versions, complaint process, actual complaint/disposition records and applicable sanctions evidence; note privacy training/designations in rows 4–5.	___ / ___ / ___
16. Individual rights: access	**D/C:** covered entity documents designated record sets subject to access and responsible office/person titles; written denials and written extension statements apply in specified circumstances. **E:** tracking supports timely processing. §164.524(b)(2), (d)(2), (e) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.524>.	Required scope/responsibility documentation and applicable correspondence; suggested request/response register. This access-focused row does not exhaust amendment, accounting, notice, or other applicable rights; counsel scopes further records.	___ / ___ / ___

Retention and preservation — not a universal log rule

Security documentation: §164.316(b)(2)(i) requires the documentation covered by (b)(1) to be retained for six years from creation or when it last was in effect, whichever is later. This does not declare a six-year minimum for every raw log or every practice record. §164.316(b)(1)–(2) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.316>.

Privacy documentation: §164.530(j)(2) applies the same six-year creation/last-in-effect, whichever-is-later starting rule to documentation required by (j)(1), subject to applicability. It is not a general medical-record retention schedule. §164.530(j) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.530>.

Recommended handling: have counsel/records owners map each record class, other applicable laws, contractual/CAP duties, and preservation holds. Do not delete merely because one period appears expired. Preserve relevant originals, versions, metadata, and actual OCR correspondence through authorized processes; identify third-party evidence and retrieval gaps. Section 160.310(c)(2) specifically addresses information exclusively held by another party that fails/refuses to furnish it; do not invent a substitute record. §160.310(c)(2) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-160/subpart-C/section-160.310>.

Addressable is not simply optional: assess whether reasonable/appropriate; implement when it is, or document why not and implement an equivalent alternative if reasonable/appropriate. No CAP-specific submissions, monitoring periods, or reporting schedules are universalized here. §164.306(d)(3) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.

Next steps

Review missing references with responsible roles, separate evidence gaps from control gaps, and route actual requests through counsel and the designated response coordinator. Do not total statuses into a compliance score or use completion as permission to launch. Share only a generic, non-sensitive summary in an introductory discussion—not evidence or PHI in booking notes.

Book a free 30-minute audit

A short introductory discussion is not a completed compliance audit or a guarantee against enforcement.

Primary official sources and editorial holds

All linked sources opened November 7, 2026 (PST). Specific subsections are identified adjacent to each checklist item. eCFR is continuously updated and unofficial; these references are not a legal opinion or exhaustive current-law review.

- Security Rule, §§164.302–164.316 <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>.
- Security documentation, §164.316 <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.316>.
- Privacy administrative requirements, §164.530 <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.530>.
- OCR cooperation/records/access, §160.310 <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-160/subpart-C/section-160.310>.
- Breach burden of proof, §164.414 <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D/section-164.414>; HHS breach guidance <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>.
- BA arrangements, §164.504(e) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.504>.
- Individual access and documentation, §164.524 <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.524>.

This is not an exhaustive responsive-production list or all-rights checklist.
No PAHL compliance status, BAA promise, capability, deliverable, privilege, or outcome guarantee asserted.