HIPAA Launch-Readiness Checklist

Seven phases, in order — every line is something OCR can ask you to produce within 10 business days. Run before launch, re-run annually and on every architecture, vendor, or state change. Engineering guidance, not legal advice.

1 · GOVERN — §164.308(a)(2) · §164.530(a) · §164.316

- [ ] Security official and privacy official designated, in writing
- [ ] Every PHI system inventoried — including logs, staging, helpdesk, push path
- [ ] Data-flow map with the BAA-covered boundary drawn and current
- [ ] Versioned written policies — one per safeguard standard, with revision history

2 · ASSESS — §164.308(a)(1)(ii)(A)–(B)

- [ ] Risk analysis covers the full inventory: threats, likelihood, impact — dated and signed
- [ ] Risk register: every risk has an owner, a decision (mitigate / accept / transfer), a deadline
- [ ] Remediation log kept, closed items dated — OCR checks follow-through, not lists

3 · CONTRACT — §164.502(e) · §164.504(e) · §164.308(b)

- [ ] BAA inventory: one row per vendor arrow on the data-flow map, signature dates filed
- [ ] Every no-BAA vendor re-architected out of the PHI path (encrypted ≠ authorized)
- [ ] Subcontractor chain verified one level down; renewal dates calendared

4 · BUILD — §164.312 · §164.310

- [ ] Unique user IDs everywhere — no shared logins; MFA on; automatic logoff set
- [ ] Encryption in transit (TLS 1.2+, DTLS-SRTP for media) and at rest (recordings, backups)
- [ ] Audit logging on PHI access; written review procedure, dated review notes
- [ ] Physical layer: workstation rules; media disposal and re-use documented

5 · TRAIN — §164.308(a)(5) · §164.530(b)

- [ ] Role-specific training at hire and on a recurring cycle — completion records dated
- [ ] Periodic security reminders sent and logged
- [ ] Sanctions policy written; applications documented (anonymized)

6 · DRILL — §164.308(a)(6)–(7) · §§164.402–408

- [ ] Incident response plan live; incident log kept — including non-breach incidents
- [ ] Breach four-factor template ready; 60-day clocks rehearsed; Part 2 dual filing planned
- [ ] Backups restore-tested with dated results; DR plan in criticality order
- [ ] Annual mock data request: fill the evidence binder inside 10 business days

7 · MAINTAIN — §164.308(a)(8) · §164.316(b)(2)(i)

- [ ] Evaluation re-run annually and on every significant change — each one a dated document
- [ ] All compliance documentation retained six years, versions kept
- [ ] Security Rule NPRM (RIN 0945-AA22) tracked: MFA, asset inventory, annual audit ahead

THE EVIDENCE BINDER — the 14 tabs OCR's first document request maps to

01 risk analysis · 02 risk-management plan · 03 policies · 04 BAAs · 05 training records · 06 sanctions policy · 07 incident log · 08 breach assessments & notices · 09 access management · 10 audit-log reviews · 11 contingency & restore tests · 12 evaluations · 13 privacy notice · 14 asset inventory & network map (proposed)