Telemedicine Audit-Log Checklist

Run before launch and before every audit. A log nobody reviews is evidence for the other side: pair every box with the review cadence. Engineering guidance, not legal advice.

1 · LOG THESE EVENTS — §164.312(b)

- ☐ Identity: logins (success + failure, method), MFA changes, role grants, every support impersonation
- ☐ Waiting room: queue join, admission (by whom), denial, transfer
- ☐ Session: per-participant join/leave with role and device, mid-call role changes, screen share, chat event (never the body), file transfers
- ☐ Recording & transcript: start (with consent reference), then every view, download, share, export, delete
- ☐ Clinical & admin: chart opens, EHR writes, config and audit-log setting changes, bulk exports, break-glass use

2 · ACCESS CONTROLS — §164.312(a) · §164.502(b)

- ☐ Unique user ID everywhere — no shared cart or front-desk logins (required specification)
- ☐ Written role matrix; each role gets its minimum-necessary slice (§164.514(d))
- ☐ Role + relationship: providers see their own patients; interpreters are session-scoped
- ☐ Support access time-boxed with ticket + reason, recorded as impersonation
- ☐ MFA on every workforce account (NIST SP 800-63B AAL2; mandatory in the proposed 2026 update)
- ☐ Auto-logoff tuned per surface; offboarding revokes access the day employment ends

3 · PROTECT THE TRAIL — §164.312(c)

- ☐ Events hold references, never PHI payloads — no chat text, diagnoses, or signed URLs in log lines
- ☐ The log is ePHI: encrypted, access-controlled, log vendor under a signed BAA
- ☐ WORM storage (e.g. S3 Object Lock, compliance mode) + hash chaining between events
- ☐ Pipeline runs on separate credentials — the production app cannot write, edit, or delete
- ☐ NTP-synchronized clocks on every service; alert on log-pipeline gaps
- ☐ Reading the audit log is itself a logged event

4 · RETENTION & REVIEW — §164.316(b) · §164.308(a)(1)(ii)(D)

- ☐ Retention policy in writing: 6 years as the federal documentation baseline; check state law, 42 CFR Part 2; ASTM E2147-18 recommends ≥10
- ☐ Cadence documented: continuous alerts → weekly triage → monthly access review → quarterly recertification → annual evaluation
- ☐ Break-glass reviewed by a human within one business day
- ☐ Every review leaves a signed record — an undocumented review didn't happen
- ☐ Memorial Healthcare: 12 months unreviewed = $5.5M. Budget review hours as OpEx

PER-SYSTEM WORKSHEET — one line per system that touches ePHI, file with your risk analysis

System _____ · Emits audit events ✓/✗ · Unique user IDs ✓/✗ · In WORM store ✓/✗ · Vendor BAA ✓/✗ · Retention _____ · Review owner _____