Telemedicine PHI-Leak Audit Checklist

Run before launch and after every new SDK, vendor, or notification template. Ten mistakes, four families — each unchecked box is an impermissible disclosure waiting for its 60-day clock. Engineering guidance, not legal advice.

1 · DATA PLACEMENT — §164.502(a) · §164.514

- ☐ URLs: no patient or clinical parameters anywhere — opaque path IDs, clinical data in POST bodies, Referrer-Policy: no-referrer on authenticated pages
- ☐ Logs and crash reports: reference IDs only, scrubbing middleware on, SDK strips request bodies and PII
- ☐ Test and staging: no production PHI — synthetic data, or a documented §164.514 de-identified extract
- ☐ CI greps routes, logs, and events for parameter names like dx, diagnosis, test, med

2 · VENDORS & BAAs — §164.502(e) · §164.504(e)

- ☐ Every system touching PHI inventoried — including helpdesk, log vendor, crash reporter, analytics, messaging
- ☐ BAA signed before the SDK ships; no BAA = public marketing site only (GA4, ad pixels)
- ☐ Recordings in cloud-BAA object storage: org-level public-access block, KMS encryption, short-lived signed URLs, every retrieval logged
- ☐ Support: structured in-app diagnostics instead of screenshots; tickets carry reference IDs only

3 · MESSAGES — §164.502(a) · (b)

- ☐ Push payloads carry nothing clinical — generic title, opaque reference; content fetched in-app after authentication
- ☐ FCM / APNs treated as uncovered carriers (they are); data-only push where the platform supports it
- ☐ Email / SMS templates: time + generic practice name + app link; no specialty, clinician, test, or medication names in sensitive verticals
- ☐ Channel preference and plain-language risk warning captured at onboarding, revocable in settings

4 · PROCESS — §164.308 · §164.404

- ☐ Risk analysis names every PHI system — logs, staging, helpdesk, push path included — dated, with a remediation log (§164.308(a)(1)(ii)(A))
- ☐ Offboarding wired to HR: same-day revocation; unique user IDs everywhere, no shared logins (§164.312(a)(2)(i))
- ☐ Quarterly access recertification; dormant accounts disabled; API keys rotated and owned
- ☐ The 60-day breach clock rehearsed: who assesses, who notifies, who documents (§164.404)

PER-VENDOR WORKSHEET — one line per vendor that touches PHI, file with your risk analysis

Vendor _____ · Touches PHI ✓/✗ · BAA signed ✓/✗ · Plan tier covers BAA ✓/✗ · PHI minimized ✓/✗ · Egress allowlisted ✓/✗ · Owner _____

Companion to: 'Common HIPAA Mistakes in Telemedicine Builds'
www.forasoft.com/learn/telemedicine-video/articles-telemedicine/common-hipaa-mistakes-in-telemedicine-builds