

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 ✓/X · BAA signed ✓/X · Plan tier covers BAA ✓/X · PHI minimized ✓/X · Egress allowlisted ✓/X · Owner _____



GO DEEPER · THE 7-VOLUME HANDBOOK

Fora Soft Video Engineering Handbook

Seven volumes, 9,000+ pages: encoding, streaming, audio and AI for video products — from the pixel to production.

By Nikolay Sapunov, CEO at Fora Soft · Kindle & paperback on Amazon

[Browse the handbook on Amazon →](#)

This checklist audits data placement, vendors and BAAs, messages and process for PHI leaks before launch. We wrote seven volumes on the video stack. Volume 7 covers compliance and regulation for AI in production, Volume 3 covers WebRTC, DRM and players, and Volume 1 covers recording and encoding.

WHAT YOU WILL FIND INSIDE

- Regulation and compliance in production
- Recording storage and access control
- WebRTC calls and secure delivery
- Real-time AI in clinical video calls

THE FULL HANDBOOK · 7 VOLUMES · 9,000+ PAGES · ALL ON AMAZON

Vol. 1 · Video Encoding — pixels and color to H.264, HEVC, AV1, quality metrics and AI

Vol. 2 · Video Streaming I — network transport, contribution and ingest, HLS, MPEG-DASH, CMAF

Vol. 3 · Video Streaming II — ABR, CDNs, players, WebRTC, DRM and the economics of delivery

Vol. 4 · Audio for Video I — PCM, codecs, loudness, accessibility, real-time voice processing

Vol. 5 · Audio for Video II — jitter buffers, lip sync, Atmos, quality metrics, neural codecs

Vol. 6 · AI for Video I — models and inference, computer vision, speech, search, generative video

Vol. 7 · AI for Video II — real-time pipelines, agents, serving, cost, compliance, verticals

Not sure your telemedicine app leaks no PHI through logs or push?

We will audit URLs, logs, vendors and notifications against HIPAA, and fix the leaks before the 60-day breach clock can start. 250+ video products shipped since 2005.

[Book a 30-min call →](#)

[WhatsApp →](#)

[Email us →](#)