Telemedicine Video Reference Architecture Pack

The component inventory, the PHI boundary, and the per-hop encryption + BAA checks on one page. Engineering guidance, not legal advice — confirm specifics with counsel.

1 · THE TEN COMPONENTS (map them before you build)

- ☐ Clients — patient & clinician apps: capture, display, in-call tools (untrusted device)
- ☐ Signaling service — agrees codecs, addresses, keys; runs over TLS
- ☐ Media server (SFU) — receives each stream once, forwards to all
- ☐ TURN relay — fallback path when a firewall blocks a direct connection
- ☐ Recording pipeline — captures & composites streams into a stored file
- ☐ Encrypted storage — recordings, files, transcripts at rest
- ☐ EHR bridge (FHIR) — reads/writes the patient's medical record
- ☐ Billing & payments — keep card data outside the boundary where possible
- ☐ Identity & access — patient proofing, clinician SSO, who sees what
- ☐ Audit & compliance — who accessed which session, when (45 CFR 164.312(b))

2 · THE PHI BOUNDARY (the line that matters most)

- ☐ Draw the boundary BEFORE choosing a single vendor
- ☐ Inside: clients, signaling, SFU, TURN, recording, storage, EHR bridge, identity, audit
- ☐ Outside, deliberately: marketing site, generic analytics, card-payment (PCI)
- ☐ Every vendor inside needs a signed BAA — coverage is binary, per vendor
- ☐ A managed vendor that won't sign a BAA cannot be inside — full stop

3 · ENCRYPTION + BAA PER HOP (two separate rules)

- ☐ Signaling over TLS; media over DTLS-SRTP (IETF RFC 3711 / 5763)
- ☐ Storage encrypted at rest; keys managed, never hard-coded in the app
- ☐ EHR write-back over FHIR on TLS; the video rarely enters the EHR
- ☐ 'Encrypted' ≠ 'compliant' — you need BOTH a BAA and encryption
- ☐ TURN relays PHI in motion → the relay vendor also needs a BAA

4 · LATENCY + BUILD-VS-BUY (same shape either way)

- ☐ One-way budget ~150 ms for natural conversation (ITU-T G.114)
- ☐ Same-region call ~140 ms: capture/encode + 2 net legs + forward + decode
- ☐ Put SFUs in multiple regions; route each patient to the nearest one
- ☐ Self-host (mediasoup / Janus / LiveKit) or buy a CPaaS — BAA still required
- ☐ Build or buy changes who runs each box, never the boundary it must respect

HIPAA §164.312 MAPS ONTO THE ARCHITECTURE (good = compliant)

The Security Rule's technical safeguards (45 CFR 164.312) line up almost one-to-one with the boxes: access control = the identity/access layer; audit controls (164.312(b)) = the audit log, which is required, not optional; integrity = backups and write protection around storage; transmission security = encryption on every hop (DTLS-SRTP for media, TLS for signaling). The contingency-plan standard (164.308(a)(7)) — a data backup plan, a disaster recovery plan, and an emergency mode operation plan — is why redundant storage and multi-region failover are part of the architecture, not extras, since availability is a named Security Rule goal (164.306(a)). Note: the 2026 HIPAA Security Rule update (NPRM 90 FR 800, RIN 0945-AA22) would make today's addressable specs mandatory and demand asset inventories and network maps that look like this diagram — proposed, not final as of mid-2026; confirm status before relying on a deadline.

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 pack puts the ten components, the PHI boundary and the per-hop encryption checks on one page. We wrote seven volumes that take each of those boxes apart. Volume 3 covers WebRTC, players and delivery economics, Volume 7 real-time pipelines and compliance, and Volume 1 the encoding inside every stream.

WHAT YOU WILL FIND INSIDE

- WebRTC and real-time media servers
- Compliance and healthcare playbooks
- Real-time latency budgets for calls
- Codec choices behind every stream

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

Need a reference architecture an auditor and your engineers both accept?

We will map your components to the PHI boundary, mark every hop that needs encryption or a BAA, and set the build-vs-buy line for each box. 250+ video products shipped since 2005.

Book a 30-min call → **WhatsApp →** **Email us →**