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.