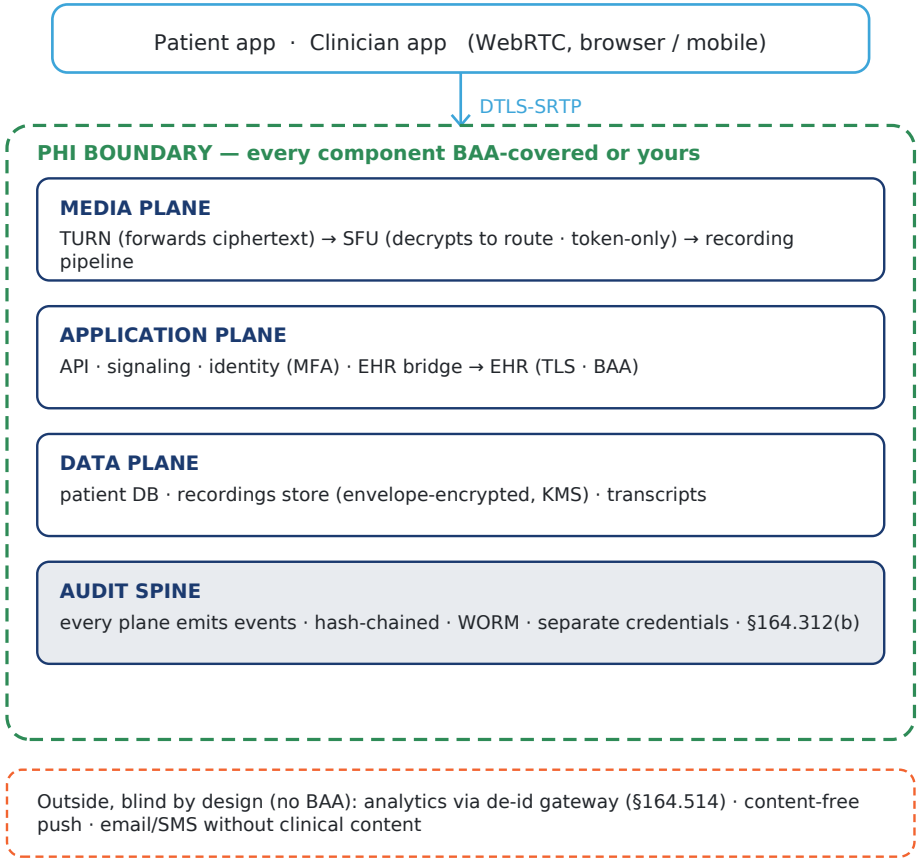
HIPAA Telemedicine Reference Architecture

The PHI boundary for a telemedicine video stack: BAA-covered components inside, encrypted hops, segmented planes, an immutable audit spine — and a blinded periphery outside.



THE SIX RULES — check what you already have

- ☐ **Draw the PHI boundary first.** Trace every data flow, including logs, crash reports, and SDKs; the map is the artifact the proposed 2026 rule requires (90 FR 898).
- ☐ **Three component kinds only.** BAA-covered, self-hosted, or blinded — encryption without a contract is still a violation (45 CFR §164.502(e); OCR cloud guidance).
- ☐ **Encrypt every hop and store; hold the keys apart.** DTLS-SRTP for media, TLS 1.2+/1.3 everywhere incl. internal hops, envelope encryption via KMS, secrets in a manager with rotation.
- ☐ **Segment four planes.** Media / application / data / admin, deny-by-default crossings; the enumerated edges are your ePHI network map.
- ☐ **Audit as a cross-cutting service.** Immutable, hash-chained, separate credentials, synced clocks; the logs are PHI and live inside the boundary (§164.312(b)).
- ☐ **PHI stays out of the periphery.** No identifiers in logs, URLs, analytics, push payloads, support tickets, or stray backups — blind what you can (§164.514).

Run quarterly: the five-minute self-audit in the article. Re-verify the 2026 Security Rule status (RIN 0945-AA22) — proposed as of 2026-06-11.