Telemedicine Video Pipeline — Security-Review Checklist

Walk every layer before a patient sees the product. Each control names its HIPAA anchor. Engineering guidance, not legal advice.

ENCRYPT EVERY HOP

- ☐ **Live call — DTLS-SRTP.** All WebRTC media encrypted endpoint-to-endpoint, no plaintext path. §164.312(e)(1)
- ☐ **Signaling — WSS / TLS.** Call setup over wss:// only; user authenticated before any call token is issued. §164.312(d),(e)(1)
- ☐ **Relay — TURN credentials.** Short-lived, per-session, and logged — never a static shared password. §164.312(a)(1)
- ☐ **Service-to-service — TLS / mTLS.** Every internal hop carrying PHI encrypted; mTLS for high-sensitivity links. §164.312(e)(1)
- ☐ **At rest — AES-256.** Recordings, transcripts, DB rows encrypted with NIST-validated modules (FIPS 140-3). §164.312(a)(2)(iv)

GUARD THE BOUNDARY

- ☐ **Routing — SFU placement.** The SFU sees plaintext PHI, so it sits inside the PHI boundary, under a BAA. §164.312(e)(1)+BAA
- ☐ **Network — segmentation.** PHI store isolated in a private subnet; no public path; narrow controlled routes. §164.312(a)(1)
- ☐ **Access — signed URLs.** Recordings served only via short-lived signed URLs; never a public bucket or permanent link. §164.312(a)(1)
- ☐ **Secrets — vault.** Keys and credentials in an encrypted vault, never in code or logs; keys stored separately, rotated. §164.312(a)(1)
- ☐ **Insiders — BAA coverage.** Every component that can see PHI is built by you or covered by a signed BAA. §164.502(e)
- ☐ **Proof — audit logging.** You can prove who accessed each recording and record, with tamper-evident logs. §164.312(b)

Remember: encryption protects data from outsiders; a BAA governs who may be an insider. PHI must pass both gates. Encrypted is not the same as compliant. Re-verify the 2026 Security Rule status (NPRM RIN 0945-AA22) — proposed as of 2026-06-14; if finalized, encryption, MFA, and segmentation become explicitly required.