Telehealth End-to-End Encryption — Decision Guide

Transport encryption already meets HIPAA. Reach for E2EE only when one of the left triggers fires — and only if you can pay the right column. Engineering guidance, not legal advice.

WHEN E2EE IS WORTH ITS COST

- ☐ **Highly sensitive care.** Behavioral health or substance-use sessions (42 CFR Part 2) where a leak would be catastrophic.
- ☐ **Untrusted infrastructure.** Parts of the media path run on hardware or in places you cannot fully vouch for.
- ☐ **Customer or contract mandate.** An enterprise, government, or international buyer requires E2EE in procurement.
- ☐ **Shrink insider / breach risk.** A small team that wants servers and staff to never be able to see consultations.
- ☐ **Otherwise: transport encryption is enough.** Routine primary, urgent, and follow-up care does not need E2EE.

WHAT E2EE COSTS YOU

- ☐ **Server-side recording stops.** The server holds only ciphertext — record on an endpoint or a named compliance recorder.
- ☐ **Transcription & AI stop.** Captions and the AI scribe read audio on the server; under E2EE they go dark unless moved on-device.
- ☐ **Browser reach shrinks.** Encoded Transform is Chrome-first in 2026; Safari/Firefox need a native app or fallback.
- ☐ **Key management is yours.** Distribute and rotate keys; lost keys mean lost data, by design.
- ☐ **Support & verification cost rises.** Encrypted calls are harder to debug; endpoints must verify keys or the guarantee weakens.

THE DECISION RULE

Ask one question of any product claiming E2EE: “can your servers technically see the media?” If yes, it is transport encryption, not end-to-end. To keep a recording under real E2EE, admit ONE named, authorized, BAA-covered, access-logged recorder as a key holder — never an open door. Never market transport encryption as “end-to-end.” Encryption is not the same as compliance: every vendor that can see PHI still needs a signed BAA.