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.



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 guide helps you decide when end-to-end encryption is worth losing server-side recording, captions and broad browser reach. We wrote a seven-volume handbook on the video stack; Volume 3 covers WebRTC, SFU media paths and DRM, Volume 7 compliance for AI features, and Volume 1 the encoding underneath.

WHAT YOU WILL FIND INSIDE

- WebRTC media paths and SFU design
- Compliance for AI captions and scribes
- DRM and protecting media in delivery
- Codec choices for encrypted real-time video

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

Deciding whether your telehealth calls need true E2EE?

We will review your media path, show where servers can see PHI today, and design E2EE with an authorized compliance recorder if you need one. 250+ video products shipped since 2005.

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