Telemedicine Threat-Model Worksheet

Run the four-step loop on every data flow. This is the engineering half of your HIPAA risk analysis (45 CFR §164.308(a)(1)(ii)(A)). Engineering guidance, not legal advice.

THE FOUR-STEP LOOP

- [ ] **1 · Model the system.** Draw a data-flow diagram: external entities, processes, data stores, flows. Mark the trust / PHI boundary — the line between what you control and everything else.
- [ ] **2 · Find threats with STRIDE.** Apply all six prompts (right) to every element and every boundary crossing. Add LINDDUN for privacy-sensitive services (behavioral, reproductive health).
- [ ] **3 · Rank by likelihood × impact.** Score each 1–5 and multiply (1–25). The top-right corner — likely and damaging — is this quarter's work.
- [ ] **4 · Mitigate, then verify.** For each high risk pick one: mitigate, transfer (BAA), accept (document it), or avoid. Then test the control — an untested control is not a mitigation.

ATTACK SURFACE — six zones to walk

- [ ] **Devices** — patient / clinician phones & laptops you don't control.
- [ ] **The live call (WebRTC)** — signaling MitM, stolen TURN credentials; SFU sees plaintext (needs BAA).
- [ ] **Signaling & API** — broken auth, broken access control, injection.
- [ ] **Recordings & data store** — public bucket, unencrypted backup, broad role. Highest value.
- [ ] **EHR & partner integrations** — leaked API key, weak partner, missing BAA.
- [ ] **Third-party SDKs** — analytics / crash / ad code shipping PHI with no BAA. Encrypted ≠ compliant.

STRIDE — apply each to every element

- [ ] **S**poofing — pretending to be someone (auth). Phished clinician login opens charts.
- [ ] **T**ampering — altering data (integrity). A dose or lab result changed in transit.
- [ ] **R**epudiation — denying an action (audit). No log can prove who accessed a record.
- [ ] **I**nformation disclosure (confidentiality). Public bucket; analytics SDK with no BAA.
- [ ] **D**enial of service (availability — itself a HIPAA duty). Flood takes the platform down.
- [ ] **E**levation of privilege (authorization). A patient account reaches an admin endpoint.

Re-run when the system changes — a stale threat model reads as negligence after a breach.
Re-verify the 2026 Security Rule status (NPRM RIN 0945-AA22), proposed as of 2026-06-14.