Telehealth Observability & Operations — Runbook

Running a live clinical-video platform: what to watch, what to alert on, and how to log without exposing patient data. Engineering guidance, not legal advice — confirm specifics with counsel.

1 · AVAILABILITY IS A HIPAA OBLIGATION

- [ ] **Treat uptime as compliance** — the Security Rule names confidentiality, integrity, AND availability of patient data (45 CFR §164.306(a)). Down = a Security Rule problem, not just an outage.
- [ ] **Have the contingency controls** — backup, disaster recovery, emergency-mode operation (§164.308(a)(7)) and an emergency-access procedure for clinicians (§164.312(a)(2)(ii)).

2 · INSTRUMENT THREE LAYERS (not just servers)

- [ ] **Layer 1 — infrastructure** — servers, databases, signaling, APIs, error rates. Necessary, never sufficient.
- [ ] **Layer 2 — real-time media, per consult** — sample WebRTC getStats() through each call: packet loss, jitter, round-trip time, resolution, frame rate. Send a per-consult quality summary; the client knows best.
- [ ] **Layer 3 — clinical funnel** — scheduled → checked in → waiting room → connected → completed → notes. A stall here is an incident even when every server is green.

3 · SET VISIT-LEVEL SLOs (what clinicians expect)

- [ ] **Objectives on the visit, not the box** — connect success ≥99.5%; time-to-connect p95 <10 s; in-call drop <1%; packet loss <2% for ≥95% of call-minutes.
- [ ] **Know your error budget** — 99.9% availability ≈ 43 min/month; 99.99% ≈ 4.3 min/month. Spend the budget on reliability when it runs low.
- [ ] **SLO ≠ SLA** — prove internal SLOs for months before promising a contractual SLA with penalties.

4 · ALERTING & ON-CALL (healthcare model)

- [ ] **Alert on symptoms, not causes** — page when connect success falls or the funnel stalls, not on raw CPU. Tune hard so a page is rare and always real.
- [ ] **Plan near 24/7** — visits run evenings, nights, and across time zones; there is rarely a window with no patient mid-visit.
- [ ] **Crisis path = highest severity** — any 988 / emergency-escalation flow gets its own monitor and top-severity alarm. It must never silently fail.

5 · LOG EVERYTHING, EXPOSE NO PHI

- [ ] **Two separate pipelines** — the HIPAA audit log records patient-data access (§164.312(b); review it §164.308(a)(1)(ii)(D); keep 6 yrs §164.316(b)(2)); operational telemetry is scrubbed of patient data.
- [ ] **Scrub at the source** — opaque user IDs only; no names, emails, MRNs, or diagnoses in URLs, error strings, traces, crash reports, or analytics (minimum necessary, §164.502(b)).
- [ ] **BAA test every tool** — a monitoring/analytics vendor that COULD see patient data needs a signed Business Associate Agreement. Encrypted ≠ compliant.

6 · DETECTION → THE BREACH CLOCK

- [ ] **Monitoring is breach detection** — discovery is the first day a breach is known, or would have been known by reasonable diligence (§164.404(a)).
- [ ] **The 60-day clock is hard** — notify affected individuals no later than 60 calendar days after discovery (§164.404(b)). Weak detection costs time, it doesn't buy it.
- [ ] **Wire detection into incident response** — the alert must trigger the documented detect → investigate → contain → notify chain.

THE ONE QUESTION IN PRODUCTION

Ask: "If a single patient on a home network can't complete a visit right now, would anything page us — and if a log line carrying a patient's name reached a third-party tool tomorrow, would we catch it?" If the honest answer to either is no, your monitoring has a hole exactly where telehealth fails. Infrastructure dashboards go green while real visits break at the edge, and patient data leaks into telemetry one harmless-looking error string at a time. Watch the visit, not the server: alert on the clinical funnel and on client-reported media quality, keep the audit log inside the boundary and the operational telemetry scrubbed of patient data, and remember that the day you should have noticed a breach is the day the 60-day clock starts whether you noticed or not. Strong, PHI-safe monitoring is what turns the worst day in production into a controlled, well-instrumented incident instead of a silent failure a clinician discovers for you.