Data Residency & PHI Location — Decision Worksheet

Classify each patient's governing regime, then place media, recordings, and backups in the right region. Engineering guidance, not legal advice — confirm specifics with counsel.

CLASSIFY THE REGIME (per patient)

- [ ] **Separate the three questions.** Residency (where data sits) vs sovereignty (whose law applies) vs localization (must stay in-region). Decide each on purpose.
- [ ] **Set the routing key.** Determine the governing regime from the patient's place of care and the provider's jurisdiction — not nationality or current travel location.
- [ ] **US patients (HIPAA).** No US-storage mandate — sign a BAA, run a risk analysis, and location is your choice (HHS Cloud Computing Q9).
- [ ] **EU patients (GDPR).** Health data is special-category; sending it out of the EU needs an Art. 45/46/49 channel. Prefer an EU region.
- [ ] **France (HDS).** EEA-only health-data hosting from Sept 2026 — a dedicated EEA region for French patients. Confirm the 24 Mar 2026 decree with counsel.
- [ ] **Canada / Quebec.** PIPEDA accountability with comparable safeguards; Quebec Law 25 needs a transfer assessment before data leaves the province.

PLACE THE DATA (per region)

- [ ] **Route live video regionally.** Put the media server (SFU) in the patient's region so the call stays local — better residency and lower latency at once.
- [ ] **Pin all at-rest PHI in-region.** Recordings, clinical records, AND every backup, replica, and analytics export live inside that region's compliance boundary.
- [ ] **Don't ship backups home.** A regional call with a single home-region backup re-creates the cross-border transfer you avoided. Backups count.
- [ ] **One control plane, many data planes.** Keep app code, routing, and deploy pipeline PHI-free and global; duplicate only the data plane per region.
- [ ] **Carry a transfer fallback.** Relying on the EU-US Data Privacy Framework? Sign Standard Contractual Clauses too — it is under appeal (Latombe, 2025).
- [ ] **Check every sub-processor's region + contract.** Transcription, analytics, recording, and storage vendors must keep regional PHI in-region with a BAA / GDPR terms.
- [ ] **Use de-identification as a pressure valve.** Properly de-identified data is no longer PHI and falls outside residency constraints — route analytics through it.

THE ONE TEST

For each patient, ask: "which single regime governs this person's data, and does any at-rest copy — recording, record, backup, replica, or export — leave that region?" If you cannot name the regime, your routing key is broken. If any copy leaves the region a localization rule pins, you have a residency violation that no encryption fixes. Settle both before launch.