Global Health-Data Law Launch Checklist

Run before launching a telemedicine product in — or selling into — any market beyond the US. HIPAA is sectoral; GDPR-family laws bind anyone processing personal data. Engineering guidance, not legal advice.

1 · MAP THE REGIMES — before any non-US launch

- ☐ Every target market listed; law classified: sectoral (HIPAA) vs omnibus (GDPR family) — the law follows the data, not the industry
- ☐ Your role named per market: controller, processor (GDPR Art. 28), PHIPA agent / electronic service provider — duties differ by role
- ☐ Health-data trigger identified: special category (GDPR Art. 9), sensitive (PIPEDA; LGPD Art. 11) — wellness data counts too
- ☐ Mandated roles appointed: EU representative (Art. 27), DPO (Art. 37(1)(c)), Quebec privacy officer
- ☐ Sector gates beyond privacy law checked: NHS DSPT + DTAC (UK), HDS hosting (France), DiGA (Germany)
- ☐ Review triggers calendared: DPF appeal C-703/25 P, EHDS milestones 2027/2029, India DPDP duties from 05/2027

2 · GDPR LAUNCH CHECKS

- ☐ Two locks recorded per processing activity in the RoPA (Art. 30): an Art. 6 basis AND an Art. 9(2) condition
- ☐ Care pathway rides Art. 9(2)(h) with Art. 9(3) secrecy duties in staff and contractor agreements — never bare consent
- ☐ Explicit consent (9(2)(a)) reserved for optional features; withdrawal path ships with the feature, per-purpose deletion works
- ☐ DPIA completed and filed before launch — large-scale special-category processing (Art. 35(3)(b)) is a textbook trigger
- ☐ Art. 28 DPA signed with every processor; sub-processor lists reviewed; same duties flowed down the chain
- ☐ 72-hour breach runbook tested end to end: detect → assess → notify authority (Art. 33); patient notice path ready (Art. 34)

3 · UK + CANADA CHECKS

- ☐ UK: UK GDPR + DPA 2018 Sch. 1 condition mapped; DUAA 2025 changes (recognised legitimate interests, ADM) reviewed
- ☐ UK: DSPT self-assessment current (CAF-aligned); DTAC evidence pack ready before the NHS procurement conversation
- ☐ Canada: express consent for health data (sensitive under PIPEDA); internal record of every breach kept 24 months
- ☐ Canada: provincial layer mapped — PHIPA/HIA agent terms signed where clinics are custodians; access requests supported
- ☐ Quebec: PIA completed and contract signed before personal information leaves the province — Toronto counts as outside
- ☐ Federal reform watched: C-27 died 01/2025, PIPEDA stands; design assuming GDPR-grade duties arrive in the successor

4 · CROSS-BORDER TRANSFER QUICK TEST — per destination

- ☐ Adequacy first (Art. 45): UK, CH, JP, KR, Canada-commercial, Brazil (since 01/2026); US only via DPF-certified importers
- ☐ No adequacy → SCCs (2021/914) signed + TIA documented (Schrems II) + supplementary measures (EU-held keys)
- ☐ France: HDS-certified host + EEA-only hosting from 09/2026 — a hosting rule that applies regardless of transfer route
- ☐ Localization mandates checked: Australia My Health Records Act s 77; India SDF negative list (reserved); Russia 152-FZ
- ☐ Remote support/admin access from third countries treated as a transfer — disclosed, safeguarded, logged
- ☐ Region pinning + per-region KMS keys asserted in infrastructure-as-code and verified by a residency test

PER-MARKET WORKSHEET — one line per market, file with your compliance records

Market _____ · Law(s) _____ · Role _____ · Contract (BAA/DPA/agent) ✓/✗ · Breach clock _____ · Transfer route _____ · Reviewed by _____ Date _____