Telemedicine De-Identification & Analytics Checklist

Run before adding any analytics tool, pixel, SDK, or data export. HIPAA recognizes de-identified — reached by two named methods — and everything else, which is PHI. Engineering guidance, not legal advice.

1 · THE THREE DOORS — every export takes exactly one

- ☐ Door 1, BAA vendor: contract signed before data flows; permitted-uses clause covers your use (incl. AI training, if any); minimum necessary applied (§164.514(d))
- ☐ Door 2, limited data set: 16 direct identifiers out, dates/town/ZIP kept; DUA signed; research, public health, or operations only — never marketing (§164.514(e))
- ☐ Door 3, de-identification: Safe Harbor (18 identifiers + no actual knowledge) or a documented Expert Determination (§164.514(b)); 'anonymized' without a method = still PHI
- ☐ Patient authorization (§164.508) used only for narrow, named secondary uses — never as a blanket analytics basis

2 · SAFE HARBOR PAYLOAD AUDIT — purge from any 'de-identified' export

- ☐ IP addresses (item O) — dropped or truncated at the edge, never stored in the export
- ☐ URLs and referrers (N) — no appointment IDs, visit types, or clinic names in paths/params
- ☐ Device IDs, advertising IDs, serials (M); phone, fax, email (D–F)
- ☐ Exact dates (C): only the year survives; ages 90+ aggregated; ZIP3 only where population > 20,000, else 000 — re-check against current Census data
- ☐ Hashed emails/MRNs fail §164.514(c)(1) — replace with random surrogate keys in a secured lookup table
- ☐ Voice (P) and face (Q): session media never leaves; export derived metrics, not recordings; free text only after redaction + expert risk assessment

3 · TWO-ZONE PIPELINE — build checks

- ☐ First-party collection endpoint on your domain; no third-party scripts inside the authenticated app
- ☐ Event allowlist enforced at ingestion: every event name + property registered and reviewed; new events ship via pull request
- ☐ Product analytics runs under a signed BAA (verify plan tier in writing) or self-hosted inside the boundary
- ☐ Marketing tags live in a separate container that cannot load in the authenticated zone; GA4/pixels on public pages only
- ☐ Aggregate exports pass small-cell suppression — every published cell ≥ 11 people (CMS precedent)
- ☐ Access to event-level data is role-scoped and logged; analytics consumers outside the boundary see numbers only

4 · RED FLAGS — stop-ship findings

- ☐ Any pixel/SDK in the authenticated app without a BAA — the GoodRx/BetterHelp/Cerebral fact pattern (FTC 2023–2024)
- ☐ Session replay capturing video tiles, chat, or form fields
- ☐ 'We anonymized it' with no §164.514(b) method named — treat as PHI
- ☐ Vendor de-identifies after receiving the data — the disclosure already happened
- ☐ Crash logs, push payloads, or support tickets carrying diagnoses or appointment details
- ☐ Expert Determination older than its stated validity, or schema changed since it was issued

PER-DESTINATION WORKSHEET — one line per external data destination, file with your risk analysis

Destination _____ · Door (1/2/3) ____ · BAA signed ✓/✗ · Payload audited ✓/✗ · Cells ≥ 11 ✓/✗ · Reviewed by _____ Date _____