Telemedicine Integration Map & Standards Checklist

One page to map every system your platform talks to, the standard on each link, and where the PHI boundary falls. Engineering guidance, not legal advice — confirm specifics with counsel.

1 · CLINICAL SYSTEMS (inside the PHI boundary — each needs a BAA)

- ☐ EHR / EMR: FHIR R4 (US Core 6.1.0 / USCDI v3, 2026) for modern reads; HL7 v2 for legacy messaging
- ☐ Scheduling: two-way sync of availability, bookings, reschedules (FHIR Appointment or iCal feed)
- ☐ Labs: orders out, results back, coded with LOINC; flag and surface abnormal results safely
- ☐ Pharmacy / e-Rx: NCPDP SCRIPT over Surescripts; EPCS adds DEA 2FA + a third-party audit
- ☐ Every clinical vendor that touches PHI has a signed Business Associate Agreement on file

2 · IDENTITY & ACCESS (the layer everything else trusts)

- ☐ Provider SSO via the hospital's identity provider (OIDC / SAML); patients via OAuth2 / OIDC
- ☐ Identity proofing matched to risk (NIST SP 800-63 IAL/AAL); EPCS prescribers proofed to IAL2/AAL2
- ☐ Provider-directory and credential sync kept current; deactivations propagate fast
- ☐ SMART on FHIR app launch (OAuth2 + PKCE) when embedding inside the EHR

3 · MONEY (keep the card path out of the PHI boundary)

- ☐ Eligibility first: X12 270/271 confirms coverage before the visit
- ☐ Claims out: X12 837P (professional) / 837I (institutional) via a clearinghouse
- ☐ Status + payment: X12 276/277 (status), X12 835 (remittance / EOB) close the loop
- ☐ Patient payments via a PCI-scoped processor (Stripe etc.) — tokens, not card data, no PHI

4 · ANALYTICS & RISK (where integration risk concentrates)

- ☐ Analytics feed is de-identified (Safe Harbor or Expert Determination) or runs under a BAA
- ☐ No PHI in logs, URLs, error trackers, or third-party tags without a BAA
- ☐ Each integration is a trust boundary: authenticate, authorize, log, and rate-limit it
- ☐ Map data direction (in / out / two-way) and the failure mode for every link before you build

THE ONE-LINE RULE

A telemedicine platform is not one app — it is a hub wired to EHRs, scheduling, identity, pharmacies, labs, billing, payments, and analytics, each speaking a different standard. Draw the map first: for every link, write down the system, the standard (FHIR / HL7 v2 / NCPDP / X12 / OAuth / PCI), the direction of data, and whether PHI crosses it. Wherever PHI crosses, a BAA is required; wherever only money or de-identified data crosses, keep it outside the HIPAA boundary. The integrations — not the video — are where most of the build cost, the timeline, and the compliance risk actually live.