Platform Anatomy PHI Worksheet

For each subsystem of your platform, answer four questions. Every unanswered row is audit scope you have not priced.

	PHI here?	BAA(s) signed?	Audit events?	Retention rule?
☐ **1. Patient & provider apps** device cache, push notifications, screenshots; WCAG 2.1 AA	☐	☐	☐	☐
☐ **2. Identity & consent** consent artifacts versioned + timestamped; MFA; NIST 800-63	☐	☐	☐	☐
☐ **3. Scheduling & reminders** appointment = PHI; reminders carry time + link, nothing clinical	☐	☐	☐	☐
☐ **4. Waiting room & triage** intake answers are PHI before any clinician is in the room	☐	☐	☐	☐
☐ **5. Real-time video core** DTLS-SRTP in transit; TURN/SFU operator inside the boundary	☐	☐	☐	☐
☐ **6. In-call clinical tools** chat, files, screen, vitals — each tool creates its own PHI store	☐	☐	☐	☐
☐ **7. Recording & documentation** recording bucket, transcript, note; un-BAA'd bucket = classic miss	☐	☐	☐	☐
☐ **8. EHR integration** FHIR R4 / US Core; the EHR owns the record, you own the visit	☐	☐	☐	☐
☐ **9. e-Rx, labs, billing** NCPDP SCRIPT, HL7 v2, X12 837/835 — PHI flows to outside parties	☐	☐	☐	☐
☐ **10. Analytics & observability** no trackers in the logged-in product; PHI filter before any SDK	☐	☐	☐	☐

Rule of thumb

One 20-minute visit leaves PHI in ~7 persistent stores (appointment, intake, chat+files, recording, transcript, note, claim). 'Encrypted' is not 'compliant': a vendor without a signed BAA is non-compliant regardless of its encryption. Addressable does not mean optional - implement it or document why an alternative is reasonable (45 CFR 164.312).