Roles, Identity & Consent Worksheet

Map your telemedicine room: who can be present, what proof each role needs, which consents must exist.

1 · The six roles - three questions each

- ☐ PATIENT - proofed per action (NIST IAL), authenticated per visit (AAL); separate consents to treatment, recording, data use
- ☐ PROVIDER - license valid where the patient sits; NPI on file; DEA registration if prescribing; credentialed
- ☐ CAREGIVER / GUARDIAN - relationship verified; legal authority per 45 CFR 164.502(g); scoped, per-category access for minors
- ☐ INTERPRETER - qualified per 45 CFR 92.201, never family by default; VRI video meets the 92.201(f) quality bar
- ☐ SUPERVISING PHYSICIAN - real-time audio-video drop-in only (CY 2026 PFS); join and leave logged
- ☐ SCRIBE / OBSERVER - workforce identity or BAA-covered vendor; patient told and agrees; AI scribes disclosed

2 · The identity ladder - step up per action

- ☐ Signup: identity attributes validated against authoritative sources (IAL1-grade)
- ☐ Sign-in: MFA available; phishing-resistant option offered (AAL2, SP 800-63-4)
- ☐ Visit: authenticated joins only; every participant role-tagged on the roster
- ☐ Prescribing: EPCS two-factor credential (21 CFR 1311.105/.115); ID-plus-selfie step-up before first prescription
- ☐ No knowledge-based quizzes where a rule sets the rung - use document + biometric evidence

3 · The consent stack - four layers, four moments

- ☐ Treatment via telehealth: captured before / at first visit, documented, consent text versioned (state laws; majority of states)
- ☐ Recording: in-session event from EVERY participant; all-party consent states covered (CA, FL, IL, MD, MA, MT, NH, PA, WA + mixed)
- ☐ Data use beyond the visit: HIPAA authorization as its own artifact; 42 CFR Part 2 consent modeled separately for SUD records
- ☐ On behalf of someone else: guardianship verified; minor-consent categories hidden from parents where state law requires
- ☐ All consents stored as append-only events: who, document version, scope, channel, timestamp; revoke = new event

4 · The join checkpoint - every role, every join

- ☐ Verify identity (step up if the role or action demands it)
- ☐ Assign a role - nobody enters untagged
- ☐ Capture the consent that covers this presence
- ☐ Announce the joiner to everyone in the room
- ☐ Write the audit event: person, role, proofing level, consent version, join/leave times

Audit dry run

Pick any minute of any visit from last quarter and answer from data alone: who was in the media session, in which role, verified at what level, under which consent version. Any blank answer is a schema gap - fix it before launch, not in discovery.