Telemedicine Authentication & Identity — Readiness Checklist

Set identity (who) and authentication (prove it) deliberately for patients and providers. Engineering guidance, not legal advice — confirm specifics with counsel.

PATIENT & PROVIDER IDENTITY

- ☐ **Separate the two dials.** Identity proofing (once) and authentication (every login) are set independently — write down the target level for each.
- ☐ **Proof patients to the risk.** IAL1 + verified email/phone for routine care; document-based IAL2 only for prescribing and other high-risk services.
- ☐ **Drop knowledge-based questions.** NIST SP 800-63-4 deprecates “previous address” quizzes — the source data is breached. Use a verified channel or document check.
- ☐ **Treat patient matching as safety.** A wrong record match exposes one patient to another — add a human review when the match is uncertain.
- ☐ **Proof providers against authoritative sources.** Checked license + national registry + credentialing; prefer SSO from the hospital identity system (see 4.8).

MFA, SESSIONS & RECOVERY

- ☐ **Build MFA in now.** The proposed 2026 HIPAA Security Rule (RIN 0945-AA22, not final as of 2026-06) would require it; it is already best practice. §164.312(d) requires authentication.
- ☐ **Choose phishing-resistant factors.** Passkeys for patients, hardware keys for staff. Offer SMS only as a last resort — NIST discourages it.
- ☐ **Pick an assurance level (AAL).** AAL2 for most access (re-auth ≤12 h / 30 min idle); AAL3 + hardware for prescribing (≤15 min idle, both factors).
- ☐ **Calibrate timeouts to the clinic.** Pair the required logout with sub-second re-auth (passkey / badge tap) so clinicians don’t defeat it.
- ☐ **Step up for sensitive actions.** Re-authenticate at the moment of signing a prescription, exporting a record, or changing a payout account.
- ☐ **Make recovery as strong as login.** Match its assurance — and keep ALL health detail out of recovery and notification messages (no specialty, no provider name).
- ☐ **Verify every identity vendor has a signed BAA.** Encryption and SSO do not replace the contract that lets a vendor touch PHI.

THE ONE TEST

Ask: “if a patient loses their phone, what does recovery require — and what does the recovery message reveal?” If recovery accepts a breached date of birth, that is your real authentication strength, not the hardware key at login. If the message names a visit or specialty, you have disclosed PHI. Fix both before launch.