Telemedicine Identity & Access Checklist

One page to scope the identity layer of a telemedicine product: patient proofing, login strength, provider SSO, the directory, and the auth-vs-access line. Engineering guidance, not legal advice — confirm specifics with counsel.

1 · PATIENT IDENTITY (proofing, NIST IAL)

- ☐ Match login to the right record — proofing, then patient matching (two steps)
- ☐ IAL1 no check · IAL2 verify real evidence (ID) · IAL3 in-person, high-risk
- ☐ Most clinical telemedicine needs IAL2 — a visit can prescribe, diagnose, bill
- ☐ Controlled-substance prescribing (EPCS) forces stronger proofing — see 4.5

2 · LOGIN STRENGTH (NIST AAL + the 2026 rule)

- ☐ AAL1 password · AAL2 multi-factor (MFA) · AAL3 hardware, phishing-resistant
- ☐ Build AAL2 (MFA) as the floor for any access to patient data
- ☐ 2026 HIPAA NPRM (RIN 0945-AA22) would make MFA mandatory — proposed, re-verify
- ☐ Never put PHI (name, diagnosis) in a JWT — it is readable, not encrypted

3 · PROVIDER SSO (no new password)

- ☐ Providers sign in via the hospital IdP — SAML 2.0 or OpenID Connect
- ☐ Inside an EHR, launch via SMART on FHIR (openid / fhirUser scopes)
- ☐ Automate provisioning AND deprovisioning with SCIM (RFC 7644)
- ☐ A departed clinician's still-live account is an audit finding and a breach

4 · PROVIDER DIRECTORY (source of truth)

- ☐ Anchor each provider to their NPI (NPPES) — an identifier, not a credential
- ☐ Verify licenses at the source (PSV via a CVO / NCQA); monitor monthly
- ☐ Model the data on FHIR PractitionerRole + Da Vinci Plan-Net
- ☐ Keep it current — ~30%/yr drift; feed the cross-state licensing check

5 · AUTH ≠ ACCESS (two layers, not one)

- ☐ Authentication = who you are; authorization = what you may see
- ☐ SSO / SMART proves identity — it does NOT grant access to every chart
- ☐ Role-based access + minimum necessary (45 CFR 164.308(a)(4) / 164.502(b))
- ☐ Log who opened which record — audit controls (45 CFR 164.312(b))

6 · BUILD OR BUY (the BAA gate)

- ☐ Don't roll your own auth — buy IDaaS or self-host a vetted platform
- ☐ If user data / tokens touch PHI, the identity vendor needs a signed BAA
- ☐ 'Encrypted' is not 'compliant' — the BAA is what makes it lawful
- ☐ Self-host (Keycloak) removes the vendor BAA but you own every control

THE ONE-LINE RULE

Proof patients to the level the riskiest action behind their identity demands (IAL2 for anything clinical) and match them to the right record; make multi-factor authentication the floor for every login to patient data, ahead of the proposed 2026 HIPAA mandate, and keep PHI out of tokens; let clinicians sign in through the hospital's identity provider over SAML or OpenID Connect and launch inside the EHR via SMART on FHIR, with SCIM switching accounts off the moment someone leaves; anchor your provider directory to the NPI, keep licenses current with primary-source verification, and feed the cross-state licensing check from it; and never confuse proving who someone is with deciding what they may see. Get those right and identity disappears; miss the directory or the deprovisioning and you find out in an audit.