Telemedicine Encryption Checklist

Run before launch and before every audit. Encrypted is not compliant: pair every box with the BAA and access-control work. Engineering guidance, not legal advice.

1 · IN TRANSIT — §164.312(e) · NIST SP 800-52

- ☐ WebRTC media on DTLS-SRTP (RFC 8827) — no custom plaintext transport anywhere
- ☐ TLS 1.2 minimum, prefer 1.3, on every signaling, API, and webhook endpoint
- ☐ Service-to-service links encrypted (TLS/mTLS) — no plaintext behind the load balancer
- ☐ TURN relays forward ciphertext; SFU decrypts — SFU treated as PHI, hardened, audited
- ☐ No PHI in SMS, email bodies, or push payloads — side channels are not encrypted

2 · AT REST — §164.312(a)(2)(iv) · NIST SP 800-111

- ☐ All seven stores inventoried: recordings, transcripts, chat/files, signaling DB, logs, backups, devices
- ☐ Object stores: server-side encryption + KMS data key (envelope) per object
- ☐ Databases: TDE / storage encryption on; logs hold no PHI (verified, not assumed)
- ☐ Laptops and phones: FileVault / BitLocker enforced by MDM, not by policy memo
- ☐ Backups and exports encrypted with the same key discipline as production
- ☐ Retired media destroyed per NIST SP 800-88 — or crypto-erased (destroy the keys)

3 · KEYS — THE SAFE-HARBOR CONDITION

- ☐ Envelope encryption via KMS; every key call authorized and logged
- ☐ Keys and data in separate failure domains — never on the same drive, repo, or account
- ☐ Root-key custody decided per store, in writing: provider / CMK-BYOK / HSM / device
- ☐ Rotation scheduled; a 'key material exposed' scenario exists in the incident runbook

4 · SAFE HARBOR & RED FLAGS — §164.402

- ☐ Breach = unsecured PHI: NIST-conformant encryption + uncompromised separate keys → loss is not reportable
- ☐ Red flag: signed URLs that never expire — the URL is the key, in plaintext
- ☐ Red flag: 'encrypted = compliant' — encryption never substitutes for the BAA
- ☐ Red flag: E2EE promised while recording / transcription / AI features are server-side
- ☐ Red flag: TLS 1.0/1.1 still answering on any endpoint a patient or EHR touches

PER-STORE WORKSHEET — one line per store, file with your risk analysis

Store _____ · Mechanism (SSE+KMS / TDE / FDE) _____ · Key source _____ · Custody: provider / CMK / HSM / device · Keys separate from data ✓/✗ · Rotation _____ · Owner _____