In-Call Clinical Tools — PHI & Consent Checklist

For each tool inside the consult: the data path, where it is stored, whether it joins the record, and the consent step. Transit is DTLS-encrypted by default — the decisions are storage, access, and consent. Engineering guidance, not legal advice — confirm specifics with counsel.

1 · SECURE CHAT

- [ ] Treat every message as PHI; encrypt at rest and access-control it like a chart entry
- [ ] Saved clinical chat joins the designated record set (45 CFR 164.501) — access + retention
- [ ] Bind each thread to a verified consult, never to a free-floating contact
- [ ] Sign a BAA with any vendor that hosts the chat store
- [ ] Accessible chat: contrast, screen-reader labels, no color-only status (WCAG 2.1 AA)

2 · FILE & IMAGE SHARE

- [ ] Write uploads to encrypted storage inside the boundary — not a generic cloud bucket
- [ ] Sign a BAA on any third-party object store that holds the files
- [ ] Lab results used clinically join the chart's retention and access rules
- [ ] Validate file types, scan for malware, and cap upload sizes
- [ ] Define a deletion path for files a patient sent by mistake

3 · SCREEN SHARE (top leak risk)

- [ ] Default to single-application / single-window sharing over full-screen
- [ ] Auto-suppress OS and app notifications while a share is active
- [ ] Show a clear 'you are sharing' indicator and a one-click stop
- [ ] Minimum necessary: never expose another patient's data (45 CFR 164.502(b))
- [ ] Close other patient charts and tabs before you start sharing

4 · ANNOTATION & LIVE VITALS

- [ ] Saved annotated images are documentation — tamper-evident, in the record (164.312(c))
- [ ] Annotation is a communication tool, not a measurement instrument
- [ ] Vitals that only display / transmit / store: low risk (FDA MDDS enforcement discretion)
- [ ] Vitals that analyze / alarm / diagnose: possible SaMD — get a regulatory read first
- [ ] Preserve device-to-display data integrity; confirm patient consent for connected devices

THE STORAGE MATH

Adding file sharing can quietly turn you into a regulated medical-image archive. Two images at ~3 MB across 200 consults a day is 2 × 3 MB × 200 ≈ 1.2 GB/day ≈ 438 GB/year — every image encrypted at rest, access-logged, and retained for your state's required years (often 6–10). Specify the encrypted store, the vendor BAA, and the retention period before you ship the upload button — not after the first audit.