RaftWorks formerly LowCodeFlow

FREE RESOURCE

THE BUILD SHEET SERIES · 02

The HealthTech Build Checklist

Health products fail reviews for the same handful of reasons — **PHI in the wrong tools, missing consent, no audit trail.** This is the checklist we work through before building anything that touches patient or wellness data, so the compliance conversation happens on day one, not launch week.

(01) Scope your data honestly

defines everything else

- [ ] **Decide: is this PHI?** Identifiable health data tied to care = PHI (HIPAA, if you serve US covered entities). General wellness data often isn't — but write the decision down.
- [ ] **List every field you collect** and cut what you don't need. The cheapest data to protect is data you never store.
- [ ] **Know your role:** covered entity, business associate, or neither — it changes which agreements you need.
- [ ] **Map where data lives:** app database, video vendor, email tool, analytics. Each one is in scope.
- [ ] **Red flag:** patient data flowing into tools that won't sign a BAA (most analytics and chat widgets won't).

(02) Consent & privacy UX

trust is the product

- [ ] **Consent at the moment of collection** — plain-language, per purpose, stored with a timestamp.
- [ ] **Separate marketing consent from care communications.** Never mix the two lists.
- [ ] **Publish how to export and delete data**, and actually build both flows before launch.
- [ ] **Minors or vulnerable users?** Add guardian consent and stricter defaults now — retrofitting is painful.
- [ ] **Intake forms collect the minimum** and mask sensitive answers from staff roles that don't need them.

(03) Architecture that passes review

what auditors look for

- [ ] **BAA-eligible vendors only in the PHI path** — video (e.g. Daily/Zoom for Healthcare), storage, email, database.
- [ ] **Role-based access:** practitioners see their patients, staff see schedules, nobody sees everything by default.
- [ ] **Audit log every access to health records** — who opened, edited, exported what, and when.
- [ ] **Encryption at rest and in transit**, short session timeouts, automatic logout on shared devices.
- [ ] **Environment separation:** real patient data never appears in dev, test, or demo accounts.

(04) Launch-day QA

run it as the wrong user

- [ ] **Try to read another patient's record** from every role — the test that matters most.
- [ ] **Book, reschedule, cancel, no-show** — the full appointment lifecycle, including every notification it fires.
- [ ] **Video visit on a bad connection** and on a phone — confirm reconnection and graceful failure.
- [ ] **Export and delete a test patient** end-to-end, and confirm the data is really gone from every system.
- [ ] **Write the incident plan:** who is notified, within what window, if data is exposed. One page is enough.
- [ ] **Ship with a kill switch:** a way to pause new bookings without taking care offline.

Building a health product?

We've shipped booking marketplaces, wellness apps with camera-based vitals, and care-reminder tools — HIPAA-aware architecture from the first wireframe.

raftworks.co/health-tech

connect@lowcodeflow.co

Not legal advice — confirm HIPAA/GDPR questions with counsel