The Pre-Flight Checklist for AI Tools

For clinics that do not have a compliance department.

How to use this. Run it before you sign, before you pilot, before a patient is in the room. Work down the list with the vendor on the call, and write the answers somewhere you can find them again.

One rule holds the whole page together: **if an answer is not in writing, it does not exist.** A reassurance in a demo is a starting point, not a fact.

1

Data and privacy, in writing

- ☐ Signed Business Associate Agreement before any data moves.
- ☐ You know where the data lives, and for how long.
- ☐ You know whether patient data trains the vendor's model, and you can opt out.
- ☐ You know how to delete a patient's data, and how to confirm it was deleted.
- ☐ Subprocessors are named.
- ☐ Audit logs exist.

2

Clinical safety: the hardest day test

If a tool needs you at your best to be safe, it is not safe.

- ☐ A clinician reviews and signs every AI output.
- ☐ You have seen how it fails on messy, real visits.
- ☐ Scope is written down.
- ☐ Care continues when the tool is down.

3

Built without us: the equity check

- ☐ You tested it on non-English visits, including code-switching.
- ☐ It works for your actual panel and their accents.
- ☐ Patient-facing pieces work for low-literacy and older patients.
- ☐ It does not help some patients while quietly failing others.

A tool demoed on clean English encounters does not fail loudly on your panel. It fails quietly. It drops the Spanish sentence. It smooths over the code-switch. Nobody flags it, because the people who would have caught it are the review team you do not have.

4

Patients

- ☐ A plain-language script in every language your panel speaks.
- ☐ A real opt-out, with no penalty.
- ☐ State recording-consent law confirmed, if it captures audio.
- ☐ Bilingual signage posted.

Need the script? *The Bilingual AI Consent Script* has the exact words in English and Spanish, the teach-back line, what to say when a patient declines, and a printable waiting-room notice. Free at drgigimagan.com/resources.

5

People and workflow

- ☐ One named owner, not a committee.
- ☐ Everyone trained, including front desk and medical assistants.
- ☐ A fast way to report failures that someone actually reads.
- ☐ Pilot before rollout: small group, fixed window, one success measure.

6

Money and exit

- ☐ Full cost known.
- ☐ Exit terms known.
- ☐ If you leave, your data comes home and theirs is deleted.

Red flags: slow down, or walk away

- ☐ No Business Associate Agreement, or the question gets dodged.
- ☐ “Trust us, it is HIPAA compliant,” with nothing in writing.
- ☐ No straight answer on whether your data trains their model.
- ☐ Designed to run with no human reviewing output.
- ☐ The demo only ever shows clean, English, textbook cases.
- ☐ Vague or verbal pricing and exit terms.

Governance-lite

You do not need a compliance department. You need one page, kept current: the tool, the owner, the adoption date, the answers above, and a short log of what failed and what you changed.

That page is your governance.

Dr. Gigi Magan, MD, MPH is a bilingual family physician and Certified Epic Physician Builder. Her work in safety-net primary care shapes how she evaluates every tool, and she writes and speaks about AI in primary care, digital health equity, and ambient documentation.

Read the newsletter: MedTech & Heart · drgigimagan.substack.com
Speaking and advisory: drgigimagan.com
More free tools: drgigimagan.com/resources