Compliance You Can't Write Your Way To

A one-page brief for the companion Lockdown Audit — HIPAA-grade data protection, scored for any business.

FACTORYOS BY COMPTRIO · YOUR DATA STAYS ON YOUR MACHINE. · COMPTRIO.COM

Most businesses handle the compliance side of AI with one line in the employee handbook: *"don't put sensitive data in ChatGPT."* It holds right up until someone does. HIPAA, attorney-client privilege, trade-secret protection — none of those are paperwork problems. They're architecture problems, and the difference only shows up at the worst possible moment.

> **The criterion:** for every safeguard, ask whether it's **enforced by the architecture** — the system won't let it be bypassed — or merely **requested by a policy** that holds only while everyone follows it. One survives a bad day, a new hire, and a vendor's terms change. The other is a promise. And underneath all of them sits one question: can anyone outside your walls read your data?

WHAT THE AUDIT DOES

It lists eight security safeguards and asks you to mark, for each, where your setup actually stands: **Built in**, **Paper only**, or **Gap**. It tallies how many are real versus promised and shows what "locked down" looks like for each. You don't have to be a hospital for this to matter — HIPAA simply spells out the strictest, best-known bar for protecting sensitive data, so it's the right yardstick for *any* business with something it can't afford to leak. Six of the eight rows map to HIPAA's five technical-safeguard categories; the last two go beyond them, to the questions that actually decide it for AI.

READING A VERDICT

- **Built in** — enforced and unbypassable. This one survives.
- **Paper only** — it exists, as a rule people must follow. One mistake or one vendor change undoes it.
- **Gap** — nothing is stopping it today. Unsure counts as a gap until proven otherwise.

THE EIGHT SAFEGUARDS

ARCHITECTURE, OR PAPERWORK?	
Least-privilege access	PAPER?
Sealed mode for crown-jewel data	GAP?
Unbypassable audit log	GAP?
Encryption at rest & in transit	BUILT IN?
No third-party read access	GAP?
Data stays on your machine	GAP?

Plus strong authentication and record integrity — eight in all. The sheet opens pre-filled with a typical cloud-AI office (mostly paper and gaps); change each row to your reality.

THE BAR IT MEASURES AGAINST

The only setup that turns **every** row into "Built in" is one where the data never leaves your machine to begin with — **nothing to disclose, nothing to egress, nothing for a vendor's terms to reach.**

THE VENDOR TEST

For each safeguard, ask any AI vendor one thing: **is this enforced by your architecture, or is it in my policy?** Then ask the question underneath all of them — **can anyone outside my walls read my data?** If the honest answer is yes, no amount of paperwork closes that gap. A vendor who can read everything your team types is a third party on every privileged conversation, and your compliance posture becomes whatever their terms say this quarter. The safeguards you can honestly mark "Built in" are the ones that hold when it counts. The rest are promises.

The companion worksheet scores all eight safeguards for your own setup and shows the locked-down target for each. Nothing leaves your computer — the point of the local, owned AI it's built for.

Sources: Comptrio, *Why HIPAA Compliance Is an Architecture Problem & Attorney-Client Privilege and AI Tools* (comptrio.com) · U.S. HHS, HIPAA Security Rule — Technical Safeguards (45 CFR §164.312).

— Shawn Snarski · FactoryOS by Comptrio · your data stays on your machine. · comptrio.com