

**“Brett — I never thought it
would happen to me.”**

— a business owner, one month after hearing a talk like this one

RxA FALL PD CONFERENCE 2026

Defend, Govern, Leverage

The Pharmacist's Guide to Cybersecurity and AI in 2026

Same tool. Different outcome. The variable is you.

Brett Gallant · Founder, Adaptive Office Solutions



DISCLOSURES

Brett Gallant

1

I have the following relationships with these commercial interests:

OWNER: Adaptive Office Solutions

2

I have received an honorarium from the Alberta Pharmacists' Association for this learning activity

3

This program has received no financial or in-kind support from any commercial or other organization

What you'll be able to do after today

- 1 Identify current cyber threats specific to pharmacy operations, and the safeguards that reduce them.
- 2 Recognize the privacy and compliance risks of unmanaged AI use, and apply basic AI governance practices in a pharmacy.
- 3 Apply a multi-perspective decision method — a “Personal AI Board of Directors” — to real decisions.

The next hour, three moves

DEFEND

What's coming at you from outside, and the layers that stop it

GOVERN

The risk you're inviting through the front door: ungoverned AI

LEVERAGE

The same tool, used with intention: your AI Board of Directors

Same tool. Different outcome. The variable is you.

What's changed in twelve months

Attacks got fluent

AI writes the phishing now. The 'bad grammar' tell is gone; it sounds exactly like your wholesaler, your vendor, your head office.

Attackers do homework

Your suppliers, your renewal dates, your people. Reconnaissance that took days now takes minutes, and they are patient.

Your data got more valuable

A complete health record is worth many times a credit card number, because you can't cancel a health record.

Two months of patience, \$400,000 gone

- 1 Day 1** Attackers get into the email system, and do almost nothing
- 2 Weeks 1–8** They watch. Learn who asks whom for money, how invoices move
- 3 The setup** Lookalike email addresses created · new phone numbers registered
- 4 The con** Stakeholders politely notified: “executives have new contact info, please update your records”
- 5 The strike** Payment requests arrive looking completely legitimate. \$400K+ lost

One word for this year: hypervigilant

The email that reads slightly off · the request that breaks the pattern · the “new phone number, please update your records.” Verifying through a channel you already trust is a security control, and it’s free.

If you OWN the pharmacy

Breach cost · liability · downtime you can’t dispense through · patient notification · whether the doors open Monday

If you WORK in it

Your name on the record that was open · your license · your reputation · your job. A breach doesn’t check who owns the building

Security is layers: the building blocks

Multi-factor everything The single highest-value lock you can turn today

Know what you have You can't protect the door you forgot exists

Patch on a schedule Most attacks use a hole fixed months ago

Backups you've tested A backup never restored from is a hope

Train your people — continually The layer attackers fear most

No single block saves you. The strength is in the stack.

The click doesn't hurt you most. The silence after it does.

Someone clicks · someone replies · someone realizes what they pasted. The most human move is to go quiet and hope it was nothing. Waiting is the one thing you can't afford — the non-profit's attackers had two silent months.

Say it before anything goes wrong:

“If you think something's off — or you think you made a mistake — tell us immediately. You will never be in trouble for reporting quickly.”

Don't raise your hand — just answer honestly



When were your backups last successfully restored — not backed up, restored?



If staff clicked something suspicious this afternoon, do they know exactly who to call?



If your email password were compromised tonight, is MFA standing between the attacker and your inbox?



Could you list every device that can reach patient information?

If one made you uncomfortable — good. That's not panic. That's your starting point.

Your staff are already using AI

Approved or not. Policy or not. Whether or not you're in the room.

SHADOW AI — the tools your people use that nobody chose, nobody vetted, and nobody governs.

“How are you using AI?”

One simple question to a manufacturing owner. The answer: staff were putting the business into a free, unvetted AI tool.

Financial statements

The customer list

Their pricing

Production reports

When it was flagged, they didn't get defensive. They changed the tool, changed the process, anonymized what they could. They saw it, and they moved.

Swap in your data

Financial statements → **Prescription records**

Customer list → **Patient names & health conditions**

Once it's in, you don't control where it goes, who trains on it, or whether it comes back out.
There is no undo button. Nobody broke in — the data left in your own hands.

Four questions with agreed answers

What's allowed

Which tools, for which tasks

What never goes in

Bright line: no patient data, no Rx records, no insurance details. Ever.

Who decides

How a tool gets approved, before it's in the workflow, not after

How data's handled

Accounts, settings, where the tool stores what you give it

Safe, unsafe, or depends?

Write a friendly refill-reminder email to a patient

DEPENDS

Safe generic; unsafe the second patient details go in

Summarize this morning's staff-huddle notes

SAFE

No patient data. Say yes to these loudly

Paste a patient's full Rx record to check interactions

UNSAFE

Every time. The bright line does not move

Help with a difficult email to an employee

DEPENDS

Strip identifying details and a 'no' becomes a 'yes'

If your pharmacy has a bad enough day —
who still has what they had this morning?

Same building. Same risk. Same side.

Your Personal AI Board of Directors

Stop asking AI for an answer. Give it five seats, five points of view, each required to disagree with the others.

The worst thing an advisor can do is tell you what you want to hear.

Each seat is a lens

1 **CFO** What does it cost, and what does it cost if we're wrong?

2 **Security Officer** Assumes it goes wrong, and asks how

3 **Pharmacist** Does this survive a real Tuesday on the floor?

4 **Future Me** A year out: did this age well?

5 **Contrarian** Argues against whatever I'm leaning toward

ACT 3 · THE EXACT SETUP — PHOTOGRAPH THIS

“You are my personal board of directors. You have five seats: a CFO, a Security Officer, a Pharmacist, my Future Self one year out, and a Contrarian. I’m going to bring you a decision. Each seat responds in its own voice, from its own priorities, and each seat must challenge at least one other seat. Do not reach consensus for me. Do not flatter me.”

The four words that turn AI from a mirror into an advisor: “Do not flatter me.”

“Should our pharmacy allow staff to use AI?”

The board derives the governance framework live, from five angles, with the weak spots circled.

Watch for each seat:

CFO

Security Officer

Pharmacist

Future Me

Contrarian

The board builds the answer live. Your job: watch which seat catches what the others miss.

The five words that make it work:

“What am I not seeing?”

Asked out loud, to something you've told not to flatter you.

ONE STORY, TOLD THREE TIMES

HEALTH

349 lbs → 130+ gone

systems · guardrails

BUSINESS

Reactive → built on purpose

systems · guardrails

TECHNOLOGY

Hoping → protected

systems · guardrails

Every one turned the same way: the day reacting stopped and the system started.

Same tool.
Different outcome.
The variable is you.

TONIGHT, NOT SOMEDAY

What to actually do

If you own a pharmacy

Adopt the one-page AI Use Policy: put the line in the sand on what never goes into a tool, before your version of that phone call.

Every single person

Build your own AI Board with the worksheet: five seats, your seats, mapped to the decisions you actually make.

One rule on every page: no patient data goes into these tools. Ever.

**Be the person who decides to be
intentional on the hard day.**

Thank you

Brett Gallant · Adaptive Office Solutions · bgallant@adaptiveoffice.ca