

KPCA ANNUAL CONFERENCE | SEPTEMBER 30, 2026

AI Agents in Healthcare

Real Tools, Real Results

Jason Mashni

Founder, Mash IT | Lexington, Kentucky

Governance, Leadership & Management track



MashIT+

THE PREMISE

Everyone in this room has used AI.
Almost nobody has used an agent.



Do you know the difference?

Your vendors are counting on you not to.

Same question. Two completely different machines.

CHATBOT / WORKFLOW



A human decided every step before it ran. Same input, same path, every time.

AGENT



The model picks the next step while it's running. The path isn't knowable in advance.

Objective one: this is the difference. Everything else in the talk sits on top of it.

Could you draw the flowchart before it ran?

YES

It's a workflow.

However many boxes it has.

NO

It's agentic.

The model chose the path.

Use this on your next vendor call.

Most “agentic” products fail it.

What I've built, and what broke

I run an MSP in Lexington. My clients are FQHCs, behavioral health practices, and other types of businesses across Central Kentucky.

I build these systems inside HIPAA environments that already exist in my clients' tenants.

Some of it worked. A lot of it broke.

FQHCs

Community health centers across Central Kentucky

Behavioral health

Practices where disclosure rules are strictest

Inside their tenants

Built in HIPAA environments that already existed

WHAT YOU'LL LEAVE WITH

- A test for any vendor claim of “agentic”
- Two use cases you could pilot without new headcount
- The governance decisions to make before you deploy
- A one-page vendor question sheet

WHAT THIS SESSION IS NOT

Not a product pitch. Nothing here is for sale.
You should leave able to evaluate vendors yourself.



USE CASE ONE

The assistant your staff already have



IN THIS SECTION

Where your data already lives

Live demo in the tenant

The permissions caveat

Your data is already in Microsoft.

If you run Microsoft 365, your documents, email, and calendars already sit inside a tenant covered by your BAA with Microsoft.

Microsoft 365 Copilot works inside that same boundary. It doesn't send your data somewhere new.

This is the one you can start using on Monday.

Enterprise tier inside your tenant — not the consumer app at the public URL.

QUESTIONS IT CAN ANSWER TODAY

- “Who's on the schedule tomorrow, and which slots are still open?”
- “What care gaps did we miss last month?”
- “Are we billing everything the provider documentation supports?”

LIVE DEMONSTRATION

Copilot inside the tenant

Real query. Synthetic scheduling data.



[Replace with screen recording]

Narrate over it. Never let the room watch in silence.

Copilot will show you how bad your permissions are.

Copilot inherits the permissions each user already has. It grants no new access.

But it makes existing overpermissioning instantly discoverable.

A file someone could technically reach but would never have found, Copilot will surface in a sentence.

BEFORE YOU ENABLE IT

- Review sharing links and group membership
- Fix the folders nobody has audited since 2019

That's not a reason to avoid it. It's a reason to fix permissions first.



USE CASE TWO

Not a voicemail



A real phone call. Synthetic patient data. A mock scheduling system.

IN THIS SECTION

Dialer vs agent

The callback demo

When someone else answers

The value case

Your EHR already calls missed appointments. That's not this.



REMINDER DIALER

- Plays a recording at a person
- Cannot hear a reply
- Cannot check the schedule
- Cannot book
- Same script every time

Outcome: a voicemail was left.

AGENT

- Has a conversation
- Hears “Thursday, but not before ten”
- Queries the schedule against that
- Proposes a time for staff to confirm
- Different path every patient

Outcome: a filled appointment.

Conversation started via  Telephony: Twilio

User

Hello?

0:01 | ASR 64 ms



Agent

 clinic-scheduling-mock_get_appointment Succeeded

0:03 | LLM 1.8 s | Tool 240 ms v



Agent

 clinic-scheduling-mock_get_patient Succeeded

0:05 | LLM 1.4 s | Tool 168 ms v

 Analyze  Report audio issue  Triage  Create test

Agent

Hi, this is Riley calling from Eastside Family Health. Am I speaking with Raymond?

0:06 | LLM 850 ms v | TTS 178 ms v



Original transcript v ...

Overview

Client data

Analysis

Workflow

Summary

+ Add tag

Send to triage

The agent, calling from Eastside Family Health, spoke with Dana, Raymond Castellanos's daughter, regarding his appointments. After verifying Raymond's date of birth, the agent informed Dana about a missed appointment on September 7th and an upcoming one on October 14th. Dana requested to reschedule the missed appointment for a Monday afternoon between 2 PM and 4 PM with Dr. Reed. The agent found an opening for October 12th at 2 PM, which Dana accepted. The reschedule request was submitted for staff confirmation. Dana then confirmed the details of the October 14th appointment. The call concluded with the agent providing confirmation of the submitted request and the clinic's contact number.

Metadata

 Copy ID vConversation ID conv_6501m28ndtg9ectahp7yjj6fa9mg 

Date Sep 11, 2026, 12:40 PM

Agent Healthcare Receptionist  Main v20Status Successful

1.0x



0:00 / 2:42



LIVE DEMONSTRATION — THE GUARDRAIL FIRING

When someone else answers the phone

Replace with second recorded call: a family member answers.



A real phone call. Synthetic patient data. A mock scheduling system.

It refuses to confirm the patient is even a patient here.

You're not overstaffed. You can't hire.

Front desk and MA roles sit open for months. The work still happens — through overtime and burnout. This covers a gap you're already carrying.

WORK IT WITH YOUR OWN NUMBERS

no-shows/week × minutes per attempt × attempts per no-show

= **hours**

× recovery rate × revenue per visit

= **recovered revenue**

Use your own numbers. I'm not going to tell you what yours are.

WHAT THE FREED TIME BUYS

- Warm handoffs for patients who need one
- Actually working the waitlist
- Being present with the person at the window

The real advantage isn't intelligence. It's concurrency.

It can call twelve people at 5:40 PM, after the front desk has gone home.

INTEGRATIONS

It has to plug into the system you already run.

MOST COMMON IN KENTUCKY PRIMARY CARE

Athenahealth

Cloud-based EHR for private practices

Elation

Clinical-first EHR platform

Greenway

AI-enabled EHR & revenue cycle

eClinicalWorks

FHIR-based EHR data exchange

Tebra (Kareo)

Cloud billing & EHR services

PLUS 100+ MORE — CONNECTOR AVAILABLE OR ON REQUEST

- Epic Systems
- Oracle Cerner
- NextGen
- Veradigm (Allscripts)
- Practice Fusion
- AdvancedMD
- Canvas Medical
- Healthie
- ModMed
- Charm EMR
- RXNT
- Azalea Health
- Dentrix
- Open Dental
- WebPT
- TherapyNotes
- Cerbo
- MEDITECH
- Practice EHR
- IntakeQ / PracticeQ
- CollaborateMD
- Netsmart
- BestNotes
- WellSky

If your system exposes an API, it can be integrated — the list keeps growing.

What else is genuinely within reach

1

Claims submission

Clearinghouses now expose transaction endpoints directly, so an agent can assemble and submit rather than a human retyping into a portal.

2

Eligibility checks

High volume, low judgment, and a standard transaction already exists for it.

3

After-hours intake

The calls that currently go to voicemail overnight and get worked the next morning, if anyone gets to them.

The pattern: wherever a standard API exists, an agent can drive it.



OBJECTIVE THREE

You're giving it real tools.
Train it like an employee.



IN THIS SECTION

Guardrails are files

Never a model decision

BAAs and the middleman

Guardrails aren't a setting. They're written instructions.

You wouldn't hand a new hire the keys and walk away. You'd tell them what to do, what not to do, and when to come get you.

An agent is the same — except the training is a document you can version, review, and hand to your compliance officer.

A compliance officer can read it.

```
agent-instructions.md
```

ABSOLUTE RULES

1. EMERGENCY. Do not assess severity.
Do not ask screening questions.
Deliver the crisis script and offer a transfer.
6. THIRD PARTIES. If someone other than the patient answers, do not confirm the patient is a patient here.

This is the whole job description. All of it.

agent-instructions.md • 3,470 words



... 3,470 words continue

THE IDENTITY GATE

“Never read the date of birth aloud. Never accept a yes-or-no confirmation of it.”

Three attempts, then it stops. It cannot be talked past.

THE EMERGENCY RULE

“Do not assess severity. If there is any doubt, treat it as one.”

The agent is forbidden from exercising clinical judgment.

THIRD PARTIES

“Being related is not the same as being authorized on the record.”

A spouse who insists still gets nothing.

Nobody reads this on a slide. That is the point — the rules live in the document, not in the demo.

Some decisions must never be the model's

1

Emergency handling

The crisis script is hardcoded and unconditional. The model never assesses severity.

2

What gets said out loud

Voicemail gives practice name and callback number. Nothing else.

3

Identity verification

Nothing disclosed until the patient states their own date of birth.

4

Writes to the record

The agent proposes. Staff confirm.

If a wrong answer could hurt a patient, a human wrote that answer in advance.

Enterprise tier: yes. Consumer app: never.



UNDER A BAA

Enterprise and API tiers of the major platforms can be brought under a business associate agreement.

Microsoft 365 Copilot, Azure OpenAI Service, and the enterprise or API offerings of the other major providers.

Verify each one directly — don't assume.

NOT UNDER A BAA

The consumer apps at the public URLs. The free tiers. Personal accounts. Browser extensions nobody vetted.

Pasting patient data into any of these is a disclosure to a vendor you have no agreement with.

Somebody in your organization is already doing the thing on the right.

Products are not HIPAA compliant. Deployments are. A vendor signs a BAA and provides controls — what you build on top is yours.

You have a third party you haven't thought about.



You'll ask whether the AI vendor signs a BAA. Almost nobody asks about the layer in between — the connector that reaches into your EHR and hands data to the model.

It needs a BAA to or build it yourself.

An MCP server is that connector: a standard way for an AI model to call your systems.

Same access questions as any vendor with a login to your EHR.

Two routes, and you own the choice

BUILD YOUR OWN

- Feasible with the API access you'll need anyway
- Full control of what data crosses the boundary
- We've done this
- Costs engineering time

USE A PLATFORM

- Integration platforms already connect to thousands of EHRs, clearinghouses, and payment processors
- Faster
- Verify their BAA posture and test against your specific EHR before you commit

Disclosure: Mash IT is a partner with one such platform, Keragon.

Partners like Keragon exist — evaluate any of them against your own environment and your specific EHR.

Monday morning

1

Find out what AI your staff are already using

Costs nothing. Usually alarming. Fastest way to get leadership attention.

2

Start with Copilot inside your own tenant

It's already under your BAA. Fix permissions first.

3

Pick one workflow with real judgment in it

If you can fully specify the decision tree, write automation instead — cheaper and easier to defend.

4

Write your guardrails before you pick a vendor

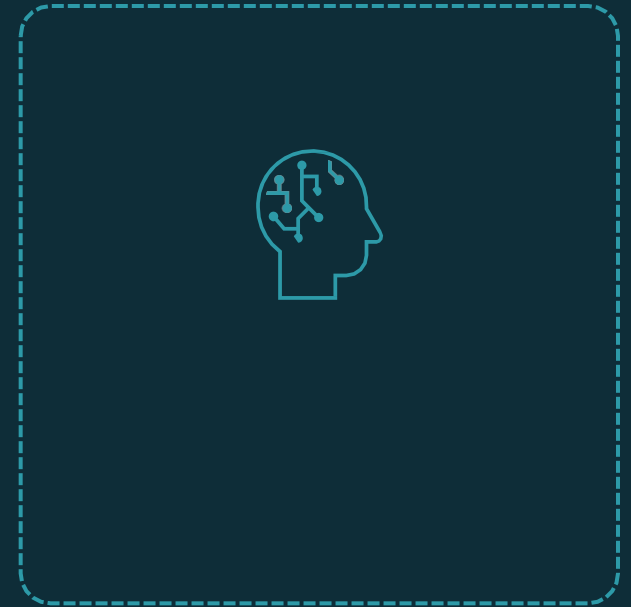
What the model may decide, what's hardcoded, what needs a human.

Take the handout. It's the questions I wish I'd asked first.

Questions



And one for you: think of the last AI product you were pitched.
Could you draw its flowchart?



Jason Mashni

Founder, Mash IT | Lexington, Kentucky

MashIT+