ClinCognition

ClinClaw

Deployment Guide

Three phases. Each one stands alone.

Audience	IT administrators, CISOs, infrastructure teams
Platform	Microsoft Teams, Azure, Epic FHIR
Risk Model	Incremental: stop at any phase
Date	March 2026
Prepared by	Ernest Pedapati, MD, Cincinnati Children's

Introduction

This document is for hospital IT administrators, CISOs, and infrastructure teams evaluating ClinClaw for deployment at their institution. It describes a three-phase rollout designed to minimize risk while delivering value at every step.

ClinClaw is an AI-powered workspace that lives inside Microsoft Teams. It connects your Epic EHR, Microsoft 365 environment, and institutional knowledge into governed workflows for both clinicians and operational staff. Unlike traditional AI vendors, ClinClaw does not require you to send data to an external cloud. It deploys as Docker containers on infrastructure you already own: your Azure tenant, your VM, your PostgreSQL instance. We ship the images. You control everything else.

ClinClaw was built at Cincinnati Children's Hospital Medical Center by a team led by a physician-engineer who lives the administrative burden it solves. It is ready for partner sites.

Why a Phased Approach

We structured deployment into three independent phases because we understand the reality of hospital IT: new systems must prove value before earning deeper integration, security reviews take time, and Epic write-back requires its own certification process. Each phase is designed to be independently valuable. Your team can stop at any phase and have a working, governed system. This is not a proof-of-concept that requires full deployment to demonstrate value. Phase 1 delivers cited document Q&A in Teams within two to three weeks, with zero patient data and zero EMR integration.

Key Principle: Graceful Degradation

Every phase is additive. Phase 1 works without Phase 2. Phase 2 works without Phase 3. Every workflow can be disabled independently. Every EMR integration can be disconnected independently. The system degrades gracefully. Disabling Epic does not break document Q&A. Disabling outreach does not break letter drafting.

This matters for your risk posture. If a capability needs to be paused during an audit, a security review, or an Epic upgrade window, you toggle one flag or remove one manifest file. The rest of the system continues operating. There is no all-or-nothing dependency.

Phase Overview

Phase	Name	Timeline	Risk Level
1	Knowledge Base + Document Q&A	2–3 weeks	Low: no patient data
2	Document Generation Workflows	2–4 weeks after Phase 1	Medium: Epic read-only
3	Clinical Write-Back + Outreach	4–8 weeks after Phase 2	Highest value and risk

Phase 1: Knowledge Base + Document Q&A

Timeline: 2–3 weeks | **Risk:** Low

The hospital uploads institutional documents (policies, SOPs, handbooks, formularies) into the RAGFlow knowledge base. Providers ask questions in Teams and get cited answers. Nothing is written back to any system. No patient data is involved.

Deployment Requirements

- Azure subscription (any tier)
- Entra ID app registration
- Teams app manifest sideloaded to a pilot group
- Linux VM or container host (ClinClaw self-hosts via Kamal on any Docker-capable machine)
- PostgreSQL database

Access Control

Entra group membership determines who can use ClinClaw. Audit logs capture every query with hashed user IDs.

Exit Strategy

Remove the Teams app. No residual data remains in any clinical system. All institutional documents stay in their original location. The RAGFlow index can be deleted from the PostgreSQL database.

Phase 2: Document Generation Workflows

Timeline: 2–4 weeks after Phase 1 | **Risk:** Medium

Adds patient letter drafting, document review, presentation generation, and leadership meeting summaries. Workflows produce DOCX/PPTX files delivered through Teams or OneDrive.

Epic Integration

SMART on FHIR with read-only scopes (**patient/*.read**, **user/*.read**). The administrator enables this independently of Phase 1. ClinClaw reads from Epic but never writes back during this phase.

Governance Controls

Control	Description
Provider Context Layers	Division leads set discipline-specific instructions without code changes
ReviewGate	human_required workflows notify providers to review output before sharing
Document Metadata	Every generated document carries workflow ID, sensitivity class, and correlation ID
Workflow Disable	Remove manifest file or toggle the enabled flag in admin panel

Phase 3: Clinical Write-Back + Outreach

Timeline: 4–8 weeks after Phase 2 | **Risk:** Highest value and risk

Pre-visit patient outreach (SMS via Azure Communication Services), appointment scheduling, and, when the institution is ready, Epic note writing.

Independent Capability Gates

Capability	Requirement	Can Be Disabled
SMS Outreach	Azure Communication Services configuration	Yes, independently
Scheduling	Epic appointment FHIR scopes	Yes, independently
Note Writing	Dedicated CLI certification against Epic sandbox	Yes, independently

Blast Radius Controls

- **Provider entitlements:** Which providers can use which workflows (Entra groups)
- **Outreach limits:** Maximum patients contacted per outreach run (manifest *outreach.maxContactsPerTrigger*)
- **Review requirements:** Whether outputs require human review before delivery (manifest *governance.reviewRequirement*)

EMR Portability

The adapter pattern means Phase 3 capabilities work with any FHIR-capable EMR, not just Epic. Switching EMR vendors requires only a new adapter. No workflow changes are needed.

What You Control at Every Phase

A common concern when evaluating AI systems is loss of control over data, access, and what the system can do. ClinClaw was designed so that your institution retains full control across four domains at every phase of deployment. Nothing is implicit. Every policy is declared in manifests that are visible in the admin panel and auditable by your compliance team.

Domain	What You Control	How
Access	Who can use ClinClaw, which workflows, who administers	Entra groups + entitlement keys
Governance	Sensitivity classification, review requirements, promotion policies, audit events	Declared in manifests, visible in admin panel
Data	Where documents are stored, audit retention, artifact metadata	OneDrive folder structure + database policy
Risk	Every workflow disabled independently, every EMR integration disconnected independently	System degrades gracefully; each capability is isolated

Infrastructure Requirements

ClinClaw is designed to run on infrastructure your institution already has or can provision through standard IT processes. There are no proprietary hardware requirements, no specialized appliances, and no vendor-managed cloud accounts. The table below summarizes what is needed at each phase.

Component	Requirement	Notes
Azure Subscription	Any tier	Used for Entra ID, container hosting, ACS (Phase 3)
Container Host	Docker-capable Linux VM	ClinClaw deploys via Kamal, single docker compose
PostgreSQL	Any managed or self-hosted instance	Stores audit logs, RAGFlow index, configuration
Teams Admin	Sideload app manifest to pilot group	No tenant-wide deployment required for pilot
Epic (Phase 2+)	SMART on FHIR app registration	Read-only scopes initially; write scopes for Phase 3
Network	Outbound HTTPS to Azure AI services	No inbound ports required beyond Teams webhook

ClinClaw deploys as Docker containers on a VM you provision. Your IT team controls the host. Your data never leaves your tenant. We ship the container images. You own everything else.

Next Steps

If your team is interested in evaluating ClinClaw, the path forward is straightforward:

- **Phase 1 pilot:** Identify a pilot group of 5–20 users in a single department. We work with your IT team to provision the infrastructure and sideload the Teams app. Timeline: 2–3 weeks to first cited Q&A response.
- **Security review:** We provide a complete architecture document, data flow diagrams, and HIPAA alignment mapping for your security team. ClinClaw has been reviewed by Cincinnati Children's information security.
- **Epic integration (Phase 2):** If Phase 1 demonstrates value, your Epic team registers a SMART on FHIR application with read-only scopes. No changes to Epic configuration beyond the standard app registration process.
- **Ongoing partnership:** We are looking for co-development partners who want to shape which workflows matter most for their institution. Your clinical and operational teams provide use-case feedback; we build and iterate.

For questions or to schedule a technical walkthrough, contact Ernest Pedapati, MD at Cincinnati Children's Hospital Medical Center.
