University of Basel
Department of Biomedical Engineering

MedMCP: An Open Agentic Ecosystem for Medical Imaging Workflows

Paul Friedrich[1,*], Julian McGinnis[2,3,4,*], Mark Muehlau[4], Jan Kirschke[4], Martin Styner[1,5], Daniel Rueckert[2,3,4,6], Philippe C. Cattin[1], Benedikt Wiestler[2,3,4]

[1] *University of Basel* [2] *Technical University of Munich* [3] *Munich Center for Machine Learning*
[4] *TUM University Hospital* [5] *University of North Carolina at Chapel Hill* [6] *Imperial College London*

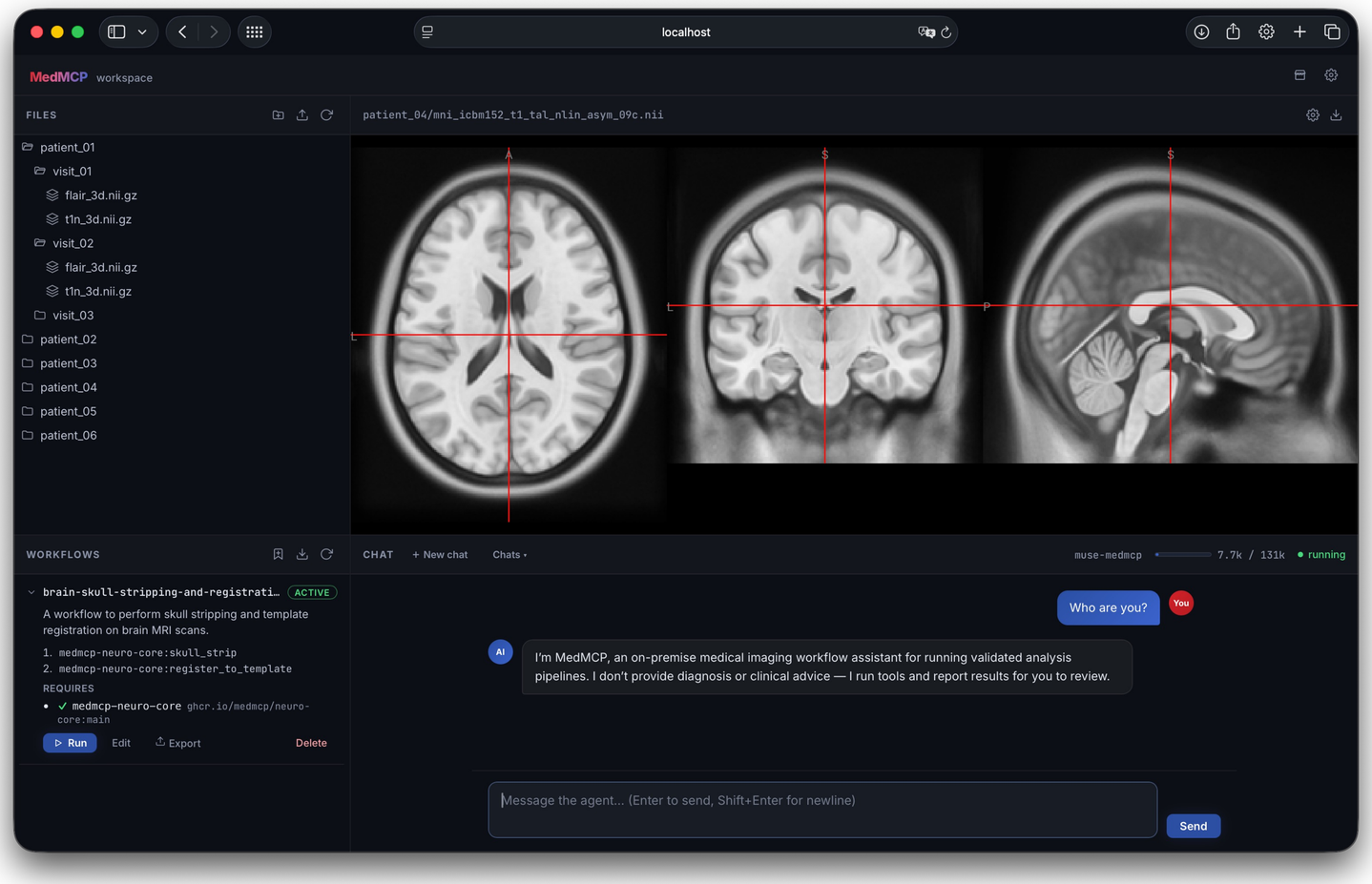
"The tools exist. The methods work. What is missing is the **infrastructure to put them in the hands of the people who are best positioned to use them**. MedMCP exists to close that gap."

① File explorer

One shared working directory. You always see the files tools read and produce.

② Image viewer

Medical image viewer for all common formats, with segmentation overlays for checking inputs and intermediate results.



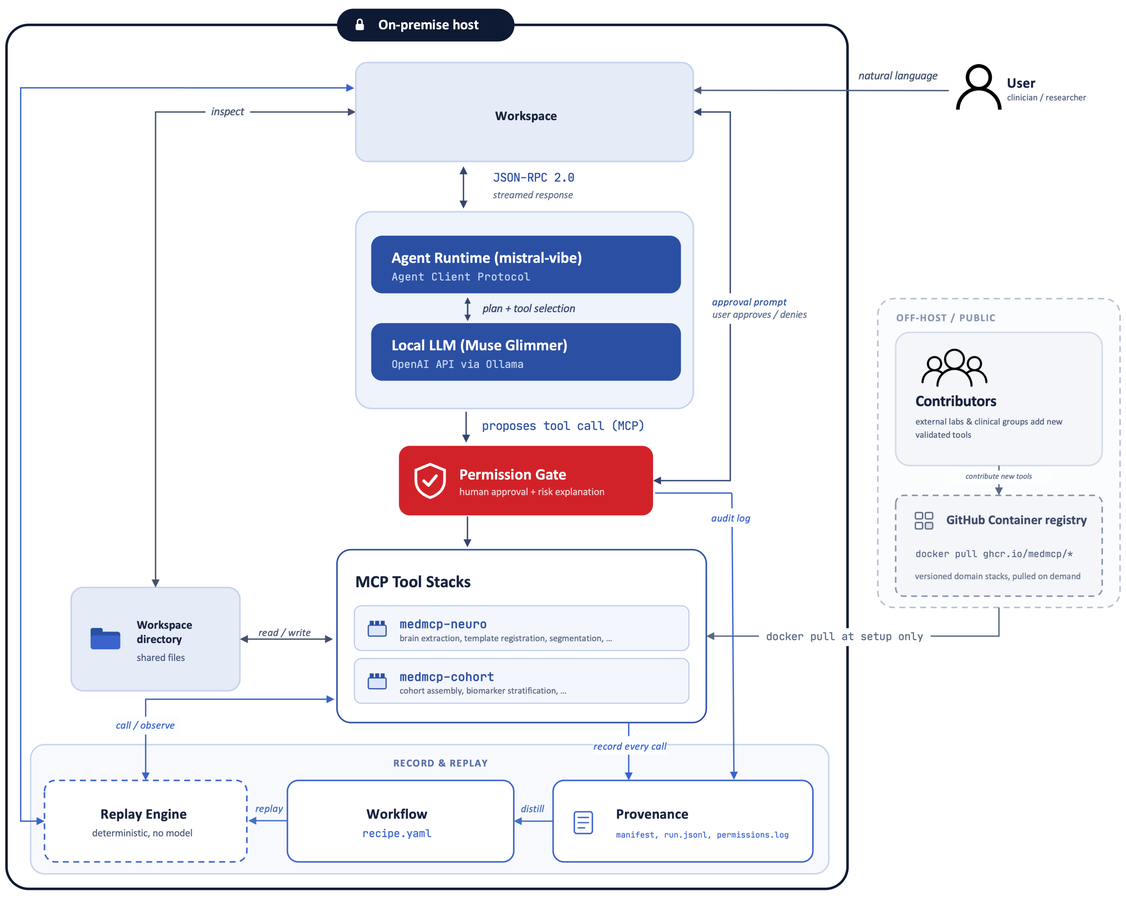
③ Replay engine

Distilled workflows re-execute without the model in the loop. Easily apply it to single cases or whole cohorts.

④ Language interface

Describe the analysis in plain language. No commands, environment management, or programming experience needed.

System architecture with orchestration/execution boundary



The Last-Mile Problem.

Validated imaging tools exist for almost every task, yet the practitioners best positioned to use them rarely can. The barrier is not capability but accumulated technical complexity: command lines, environments, file formats, APIs. MedMCP closes this gap by exposing imaging tools through natural language.

MedMCP's Design Principles.

Bounded. The agent **only invokes pre-validated tools.** It never generates code on the run.

Gated. Every side-effecting call passes a **human-in-the-loop permission gate.** No auto-approval path.

Auditable. An **append-only provenance record** links every output to the tools, parameters, and inputs that produced it.

Local. **Everything runs on-premise.** No imaging data, metadata, or results ever leave the institution.

Get Involved.

MedMCP is built as a **community-driven ecosystem.** We are actively looking for contributions and call for an MCP server to become a **standard release artifact of all method papers.**

Website:

Partner Institutions:

Munich Center for Machine Learning
Universitäts Klinikum
The University of North Carolina at Chapel Hill
IMPERIAL