



Where pharmaceutical AI needs an execution boundary

The useful question is not only whether an AI system performs well. It is whether a particular proposed action is authorized, within scope and permitted under the applicable policy at the moment of execution.

SIX WORKFLOW HYPOTHESES FOR DESIGN-PARTNER EVALUATION

DEVIATION / CAPA

Proposed action: Open, classify or route a record

Decision question: May this agent act for this site, product and severity?

Evidence focus:
Request, authority, rule and outcome

CHANGE CONTROL

Proposed action: Initiate a change or assessment

Decision question: Is it inside delegated authority and approved scope?

Evidence focus:
Scope, approval path and decision

GXP RECORDS

Proposed action: Create or modify controlled data

Decision question: Is this exact record action permitted now?

Evidence focus:
Actor, record, policy and result

REGULATORY OPS

Proposed action: Route or submit regulated content

Decision question: Who holds authority for this jurisdiction and artifact?

Evidence focus:
Submitter, artifact, policy and verdict

SUPPLIER QUALITY

Proposed action: Open an investigation or restrict status

Decision question: Do evidence, role and policy support the restriction?

Evidence focus:
Evidence basis, authority and outcome

CROSS-SYSTEM AGENT

Proposed action: Read in one system; act in another

Decision question: Does purpose-bound authority survive the boundary?

Evidence focus:
End-to-end intent and decision chain

Illustrative hypotheses for discovery. Each workflow requires customer-specific quality, validation, security and regulatory assessment.



The control pattern

ExecLayer is designed to sit outside the model as a separate authority boundary. The model may propose an action; execution depends on a deterministic decision.

1 PROPOSED INTENT

Operation, target, actor, purpose and context

2 CANONICAL ACTION

The request is normalized into an exact action blueprint

3 POLICY + AUTHORITY

Rules, permissions, grants, limits and approval requirements are evaluated

4 ALLOW / REFUSE / ESCALATE

Only a cleared action may reach the execution adapter

5 AUTHORITY RECEIPT

The decision is bound to the request and governing policy as signed evidence

WHAT AN EVALUATION SHOULD PROVE

- The action is intercepted before an external side effect.
- Authority and scope are evaluated independently of model reasoning.
- The same request and rules produce the same decision.
- Denied actions cannot bypass the execution boundary.
- Receipts preserve the request, policy version and outcome.

WHAT EXECLAYER DOES NOT CLAIM

- Automatic GxP compliance or regulator approval.
- Replacement of accountable human oversight.
- Replacement of CSV, QMS, IAM, cybersecurity or audit controls.
- Suitability for a specific workflow without validation and risk review.

Proposed next step: map one bounded workflow

Output: a workflow control map, named authority owner, integration boundary, evidence requirements and a decision on whether a bounded evaluation is justified.

Tyler Strause-Tabares | VP Business Development | tyler@execlayer.io

