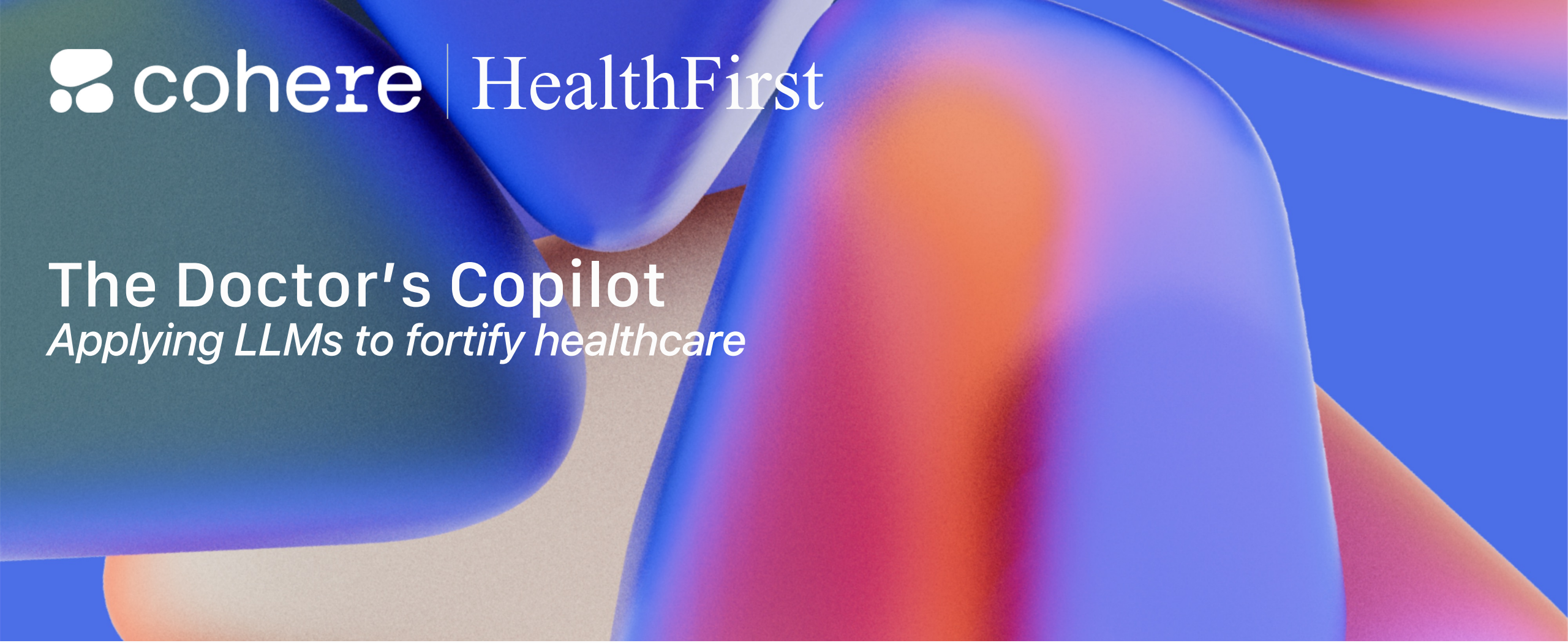


The Doctor's Copilot

Applying LLMs to fortify healthcare

Neel Gokhale
neelg14@gmail.com

May 10, 2024

Agenda

1	Understanding the problem	Slide 3
2	Solution overview	Slide 4
3	Key considerations	Slide 5
4	Technical architecture	Slide 6
5	POC demo	Slide 8
6	Next steps	Slide 10

Understanding the challenges

Data is ubiquitous, yet disparate and non-standard

- → The healthcare industry grapples with data fragmentation stemming from diverse sources, formats, and quality standards, hindering seamless integration and comprehensive analysis.
- → Lack of standardized data formats and inconsistent quality impede efficient data utilization and downstream analytics

☞ Kruse et. al.

Traditional LLM systems may fall prey to unreliability

- → Although LLM adoption is desired, concerns persist regarding their accuracy and the uncertainty of their output, potentially impacting reliable clinical decision-making.
- → Despite advances in context-enhancement techniques, such as RAG, the criticality of clinical decision making requires more robust methodologies to evaluate even the context that is generated

☞ Ahmad et. al.

Data privacy dictates the adoption of tech in healthcare

- → Healthcare organizations face stringent regulatory requirements, such as PIPEDA and HIPAA, to safeguard patient data
- → Balancing the imperative of data access for medical innovation with stringent privacy regulations poses a delicate challenge, necessitating policies and safeguards to mitigate exposure

☞ HIPAA Guidelines

Solution overview – how Cohere aims to address the 3 core challenges

Data is ubiquitous, yet disparate and non-standard

Leverage Knowledge Graphs as the core structure to consolidate, correlate and index disparate data

- → Knowledge graphs structure data into interconnected nodes and edges and allow more nuanced information retrieval than linear semantic/lexical searches.
- → LLMs can easily synthesize "entity-relationship-entity" chains that succinctly convey the context with minimal added tokens.
- → Graph-RAG shows strong potential in the medical sector based on emerging research

☞ Jiang et. al. (HyKGE)

Traditional LLM systems may fall prey to unreliability

Use corrective-RAG through a well-defined state-machine flow to ensure a robust and methodical pipeline

- → Corrective-RAG is a methodology used for evaluating the confidence and reliability of context before response generation
- → By incorporating a well-defined state-machine flow, the solution ensures a systematic evaluation of retrieved context.
- → CRAG also amends inadequate context with additional documents from vetted external sources (PubMed)

☞ Yan et. al. (CRAG)

Data privacy dictates the adoption of tech in healthcare

Build a self-contained solution using Cohere's private deployment offering and apply PHI guardrails

- → Cohere's private deployment offering allows for the creation of self-contained solutions hosted within the healthcare organization's infrastructure, providing greater control over data privacy and security
- → PHI guardrailing mitigates the risk of data exposure and LLM tracing provides the auditability for complex black-box systems

☞ Cohere

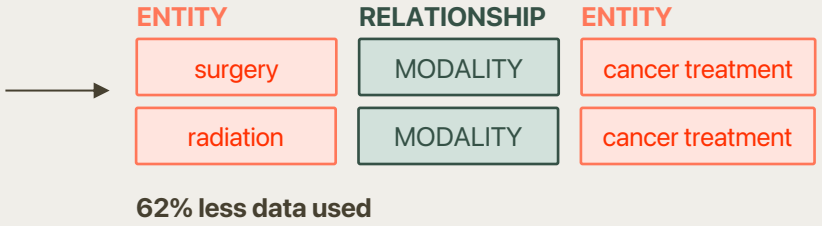
Solution overview – privacy considerations

Data

- While data anonymization is a key aspect of complying to privacy standards, **data minimization** is also an important mitigation approach *HIPAA 164.502(a)(1)*
- Condensing large chunks of unstructured data into chains of essential information in the KG builds onto this concept
- The sensitivity of the data that HealthCare wants to leverage impacts the disclosure, retention and usage policies *PPIEDA P5*

RAW DATA PACKET

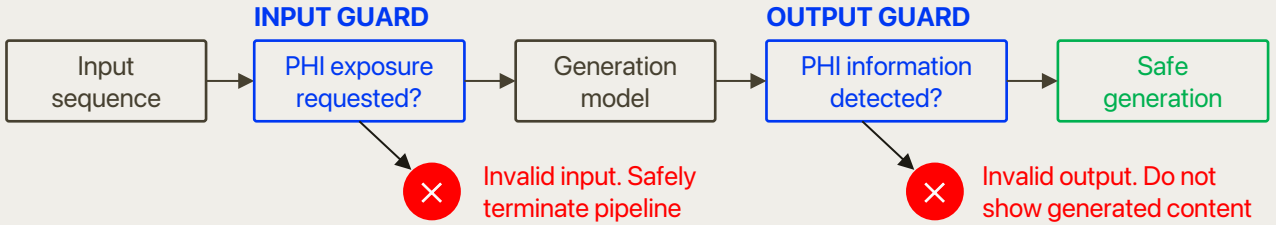
Traditional cancer treatment modalities, including surgery and radiation, have made significant strides in improving patient outcomes.



62% less data used

Model

- We apply input and output guardrailing to the main generation model to mitigate data penetration and exposure
- Apply Cohere Classify to terminate generation if **an input** sequence asks for PHI or irrelevant information
- Train/prompt Command to mask any PHI **in output** for **18 classes** defined by HIPAA to comply with the Safe Harbor standard *HIPAA 164.514 & PPIEDA P7*



Technology

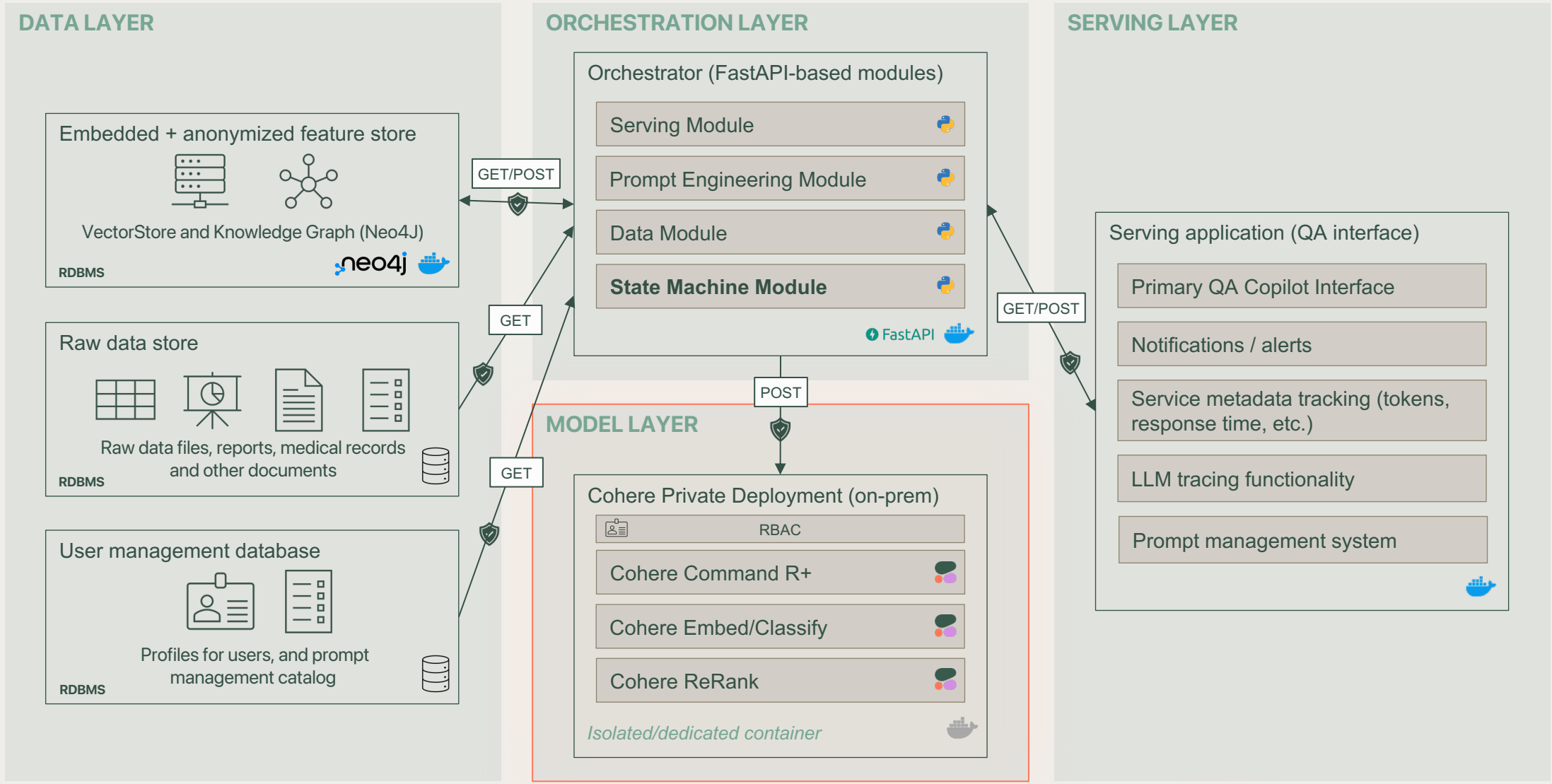
- Cohere has 3 model deployment offerings that will cater to the needs of their clients. The key dimensions are **data privacy and integration**
- Depending on the nature HealthFirst's data, the Cloud VOC or Private Deployment options are lucrative
- Our preliminary recommendation is the Private Deployment offering, given that PHI data may be leverage

SaaS	Integration w/ Cloud VOC	Private Deployment
Quick and easy	Integration into existing cloud environment	For customization and control. Can be deployed on-cloud or on-prem
Best for: low-scale experimentation and pilot dev	**Best for:** tech stacks that actively leverage cloud services	**Best for:** highly sensitive data that needs control

Preliminary recommendation

HIPAA - Health Insurance Portability and Accountability Act
PIPEDA - Personal Information Protection and Electronic Documents Act

Target-state solution architecture*

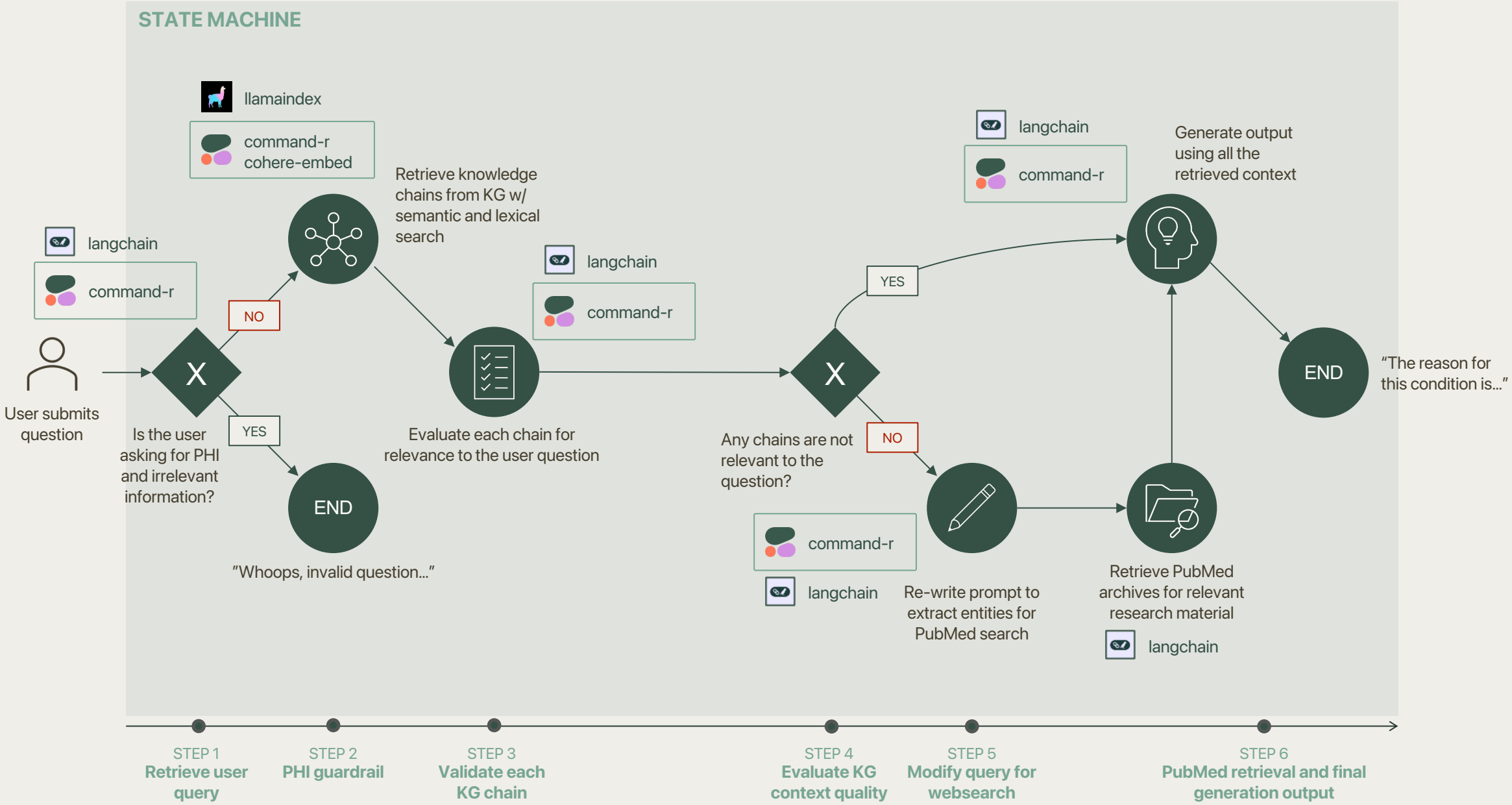


*This is a proposed solution architecture based on a preliminary understanding of HealthCare's tech stack and is subject to change pending further analysis

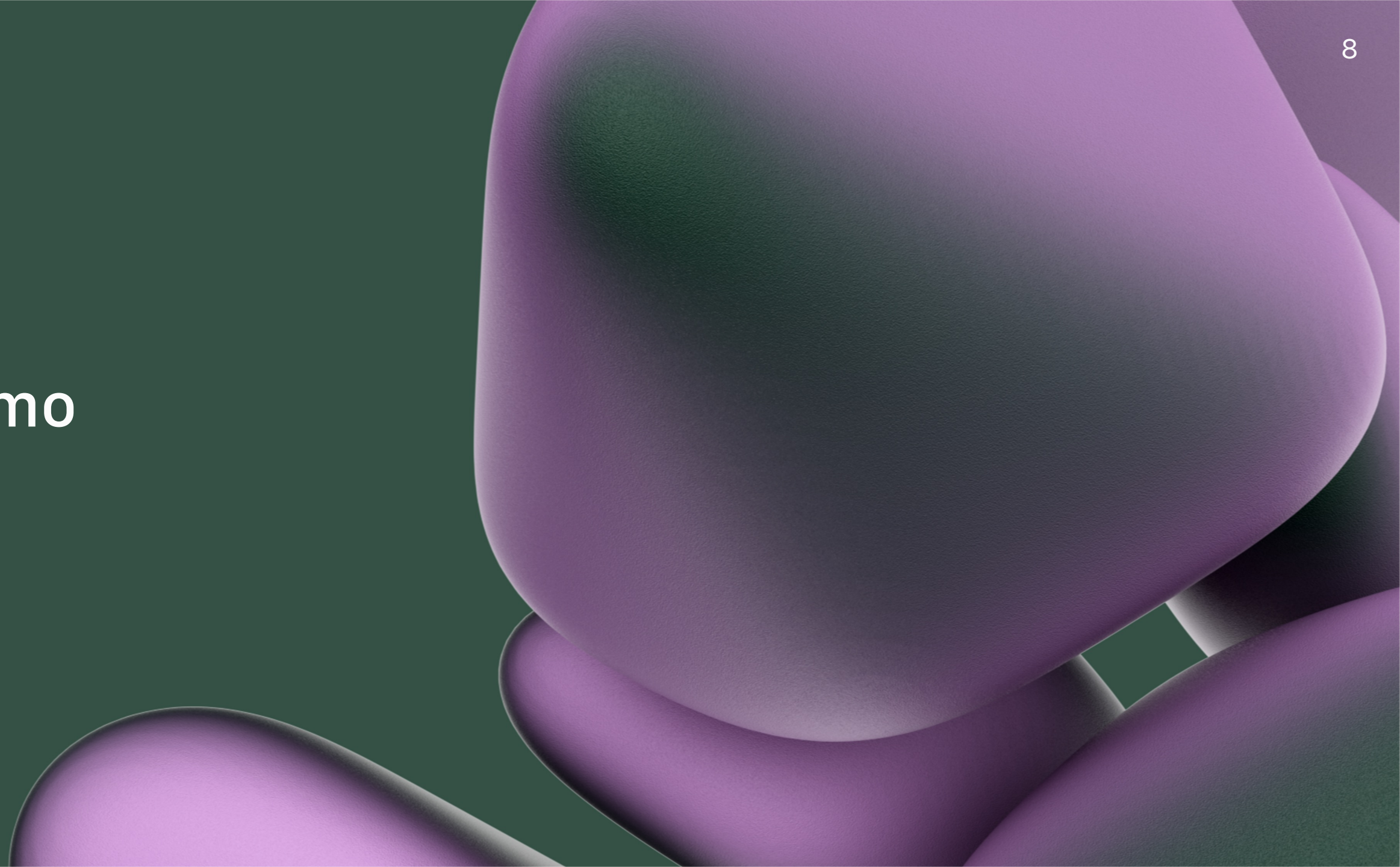
New components we would bring

Components built into existing infra.

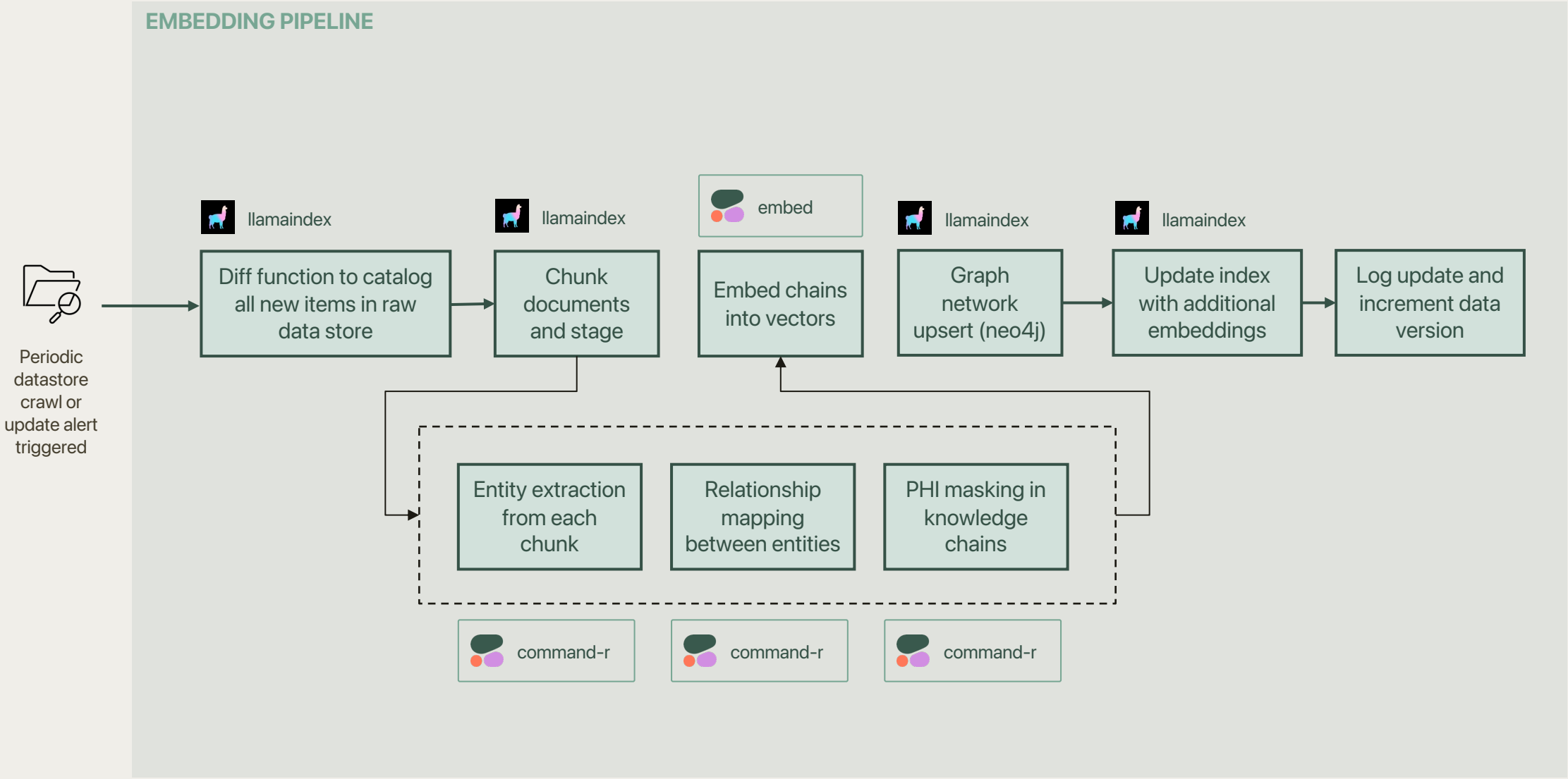
POC state machine – high-level flow (@ inference time)



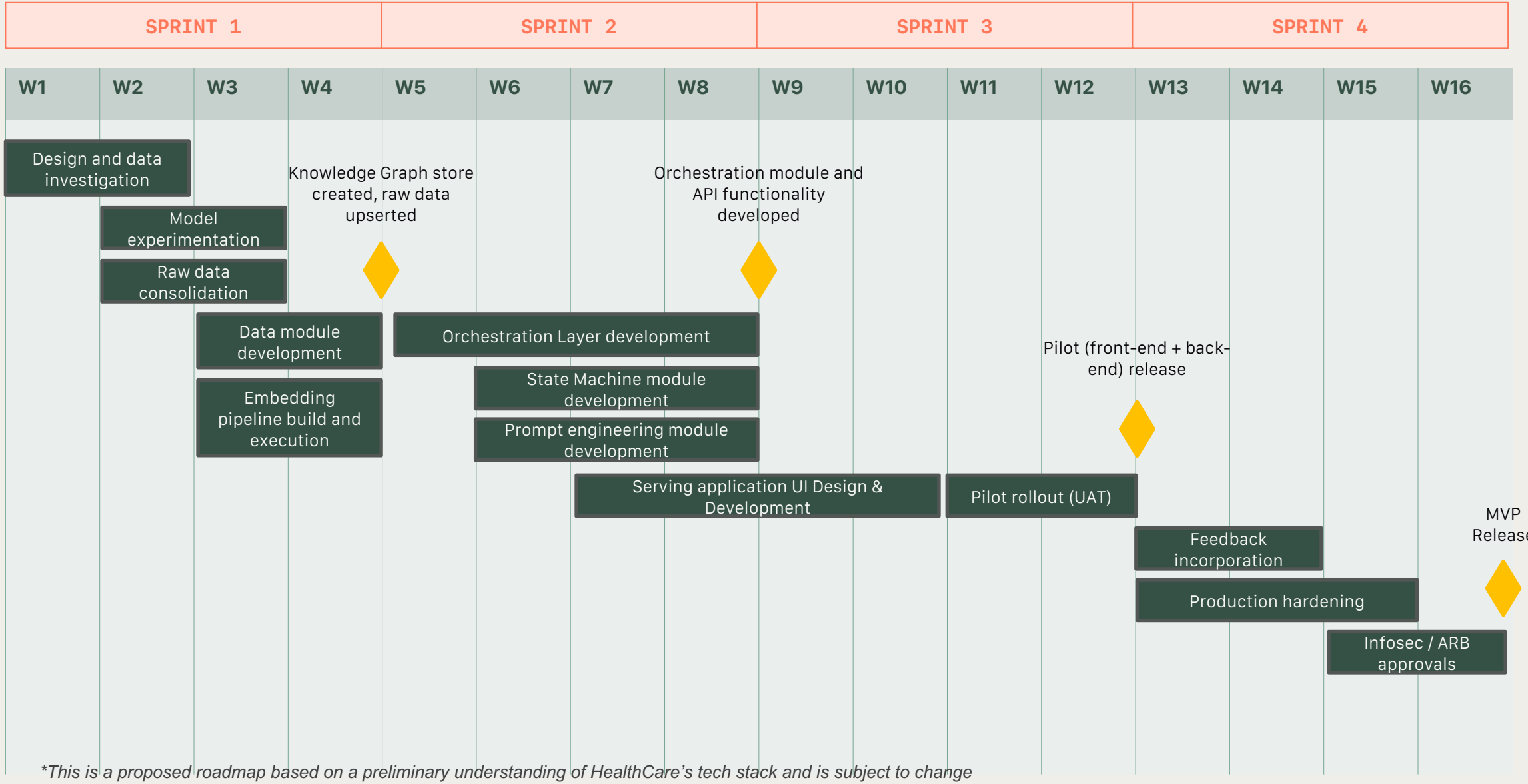
Demo



Embedding pipeline – high-level flow (periodic staged process)

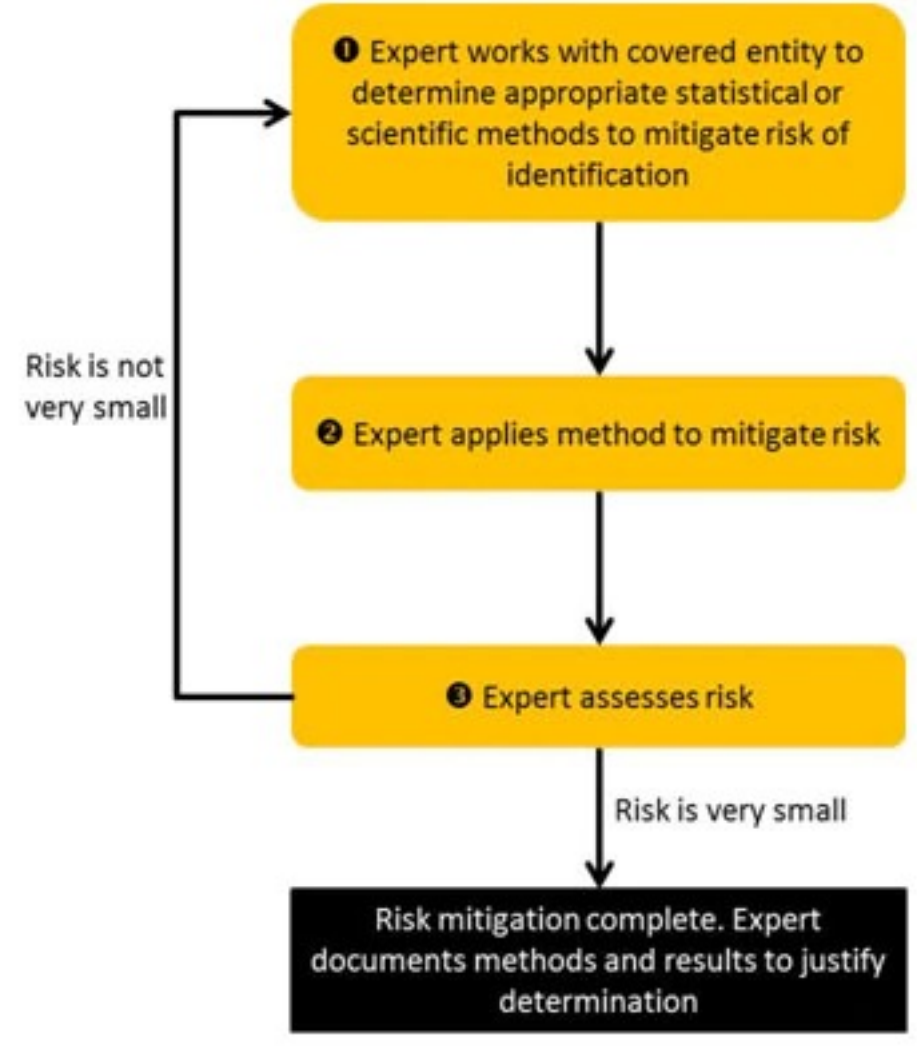


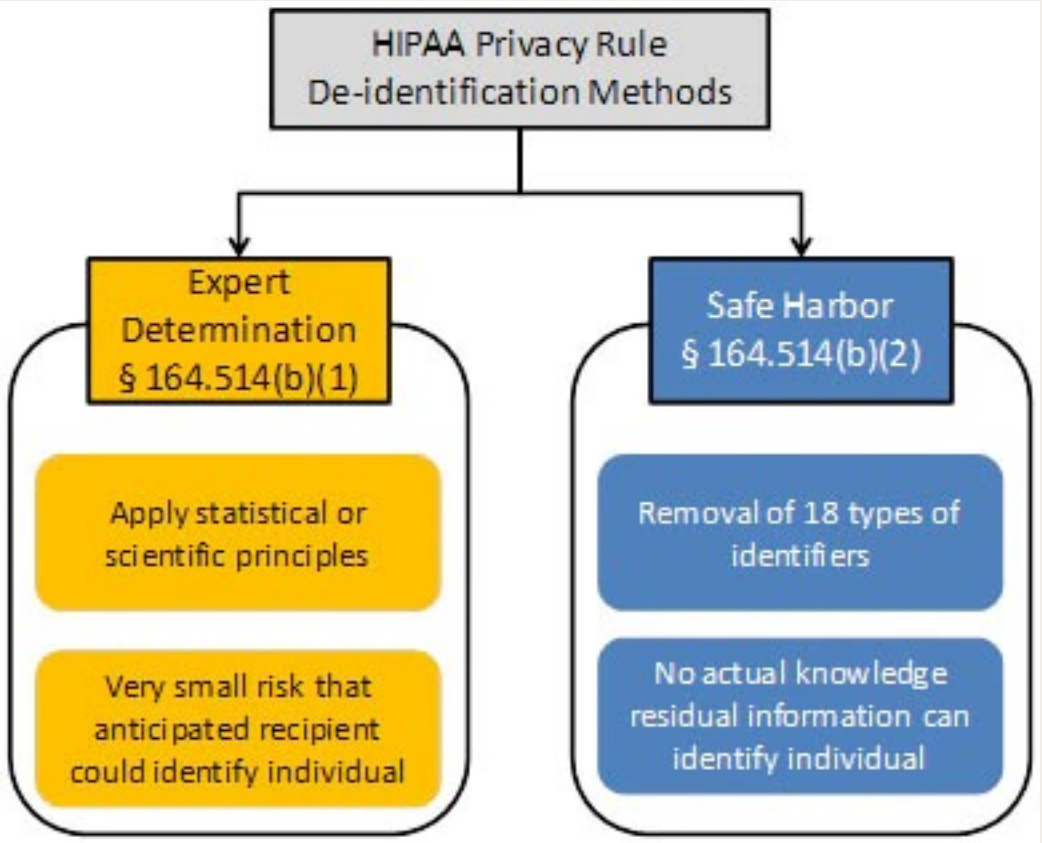
Proposed delivery roadmap



*This is a proposed roadmap based on a preliminary understanding of HealthCare's tech stack and is subject to change pending further analysis

HITL approach for vetting privacy-enhancement guardrails





[HIPAA Guidelines]