# HealthLLM Chatbot MVP Project

*Design and Evaluate a Domain-Specific Chatbot with Ollama + AnythingLLM*

## Project Overview

In this project, you will be **randomly assigned a specific healthcare scenario**. You will build a **Minimum Viable Product (MVP)** LLM-powered chatbot designed to support that scenario, using **RAG (Retrieval-Augmented Generation)** and **System Prompt** engineering techniques on a local framework.

> ⚠ You will **not** train your own model. Your goal is to **design, configure, and test**:
> ☑ A well-curated, scenario-specific **Knowledge Base**.
> ☑ A precise **System Prompt** defining the chatbot's role, tone, and ethical boundaries.

## Project Goals

| Goal | Description |
|---|---|
| **Understand the design of conversational AI in sensitive domains** | Including user needs, scenario constraints, and compliance requirements. |
| **Master the RAG pipeline** | From data collection → cleaning → indexing → usage in AnythingLLM. |
| **Craft high-quality System Prompts** | Clearly define role, tone, scope, and ethical boundaries. |
| **Identify and mitigate ethical risks in healthcare AI** | Including crisis response, privacy protection, and disclaimers. |

## Provided Technology Stack

| Component | Purpose | Notes |
|---|---|---|
| **Ollama** | Local LLM backend (e.g., Mistral, LLaMA) | CLI-based, downloads and runs models locally. |
| **AnythingLLM** | Front-end and RAG management | Supports document upload, indexing, prompt management. |
| **Tutorial Materials** | Quickstart guides & demos | Setup instructions, troubleshooting tips. |

## Scenario Materials

Each student will receive a **"Scenario Pack"** (Markdown) containing:

| Field | Example | Description |
|---|---|---|
| **Scenario Description** | “Managing Mild Anxiety for College Students” | Background context, user needs, constraints. |
| **Target User** | Undergraduate students experiencing mild anxiety | May include demographic details. |
| **Conversation Goal** | Identify stressors & suggest evidence-based coping strategies | Defines what success looks like. |
| **Chatbot Role** | “Friendly, supportive wellness coach” | Define the role that the chatbot will play. |
| **Test Questions** | 2 standard test questions | Used for evaluation. |

## Task Breakdown

### 1 Read Your Assigned Scenario Pack

- Produce a clear `use_case_description.md` that identifies user pain points and success criteria.

### 2 Prepare the Knowledge Base

- Collect highly relevant, evidence-based resources (e.g., clinical guidelines, hotline information, authoritative blogs, etc.).
- Clean and format these as PDF/Markdown/TXT compatible with AnythingLLM.
- Emphasize clarity, focus, and utility.

### 3 Design Your System Prompt

- Must include:
  - Explicit role definition and tone (e.g., warm, non-judgmental).
  - Scope limitations.
  - Required disclaimers (e.g., "Not professional medical advice").
  - Crisis-response instructions (e.g., self-harm triggers emergency help suggestions).
- Iterate: test and refine for clarity and alignment.

### 4 Integration and Testing

- Upload documents and prompt in AnythingLLM.
- Bind the model and run realistic conversation tests.
- Record transcripts and refine as needed.

### 5 Submission

- Push all materials to a **GitHub repository**.
- Prepare a demonstration video (no more than 2 mins)
- Be ready for a 5-minute presentation session.

---

## Expected Deliverable Structure

```
/healthcarellm-chatbot-mvp
├─ knowledge_base/
│  ├─ knowledge_document_1.pdf
│  ├─ knowledge_document_2.md
│  └─ knowledge_document_3.txt
├─ prompt/
│  └─ system_prompt.txt
├─ documentation/
│  └─ scenario_pack.md (Provided)
│  └─ use_case_description.md
├─ demo/
│  ├─ demo_video.mp4
│  └─ chat_transcript.txt
└─ README.md
```

> **The chatbot README.md file must prominently display a "Not Medical Diagnosis" disclaimer.**

## Grading Rubric

| Criterion | Description |
|---|---|
| **Knowledge Base Relevance and Quality** (20 points) | 1. Curates highly relevant, evidence-based documents tailored to the assigned scenario.<br>2. Ensures clean, structured, AnythingLLM-compatible formatting.<br>3. Demonstrates clear focus without irrelevant content, with explained selection rationale. |
| **System Prompt Design and Ethics** (20 points) | 1. Explicitly defines chatbot role, tone, functionality, and boundaries.<br>2. Includes mandatory disclaimers and crisis-response guidance.<br>3. Shows understanding of ethical risks and integrates safeguards. |
| **Integration and Testing in AnythingLLM** (20 points) | 1. Successfully uploads and configures the knowledge base and prompt.<br>2. Conducts realistic test conversations simulating user queries.<br>3. Documents and iterates design based on test results. |
| **Documentation and Reflection** (20 points) | 1. Clearly describes use case, user group, goals, and ethical considerations.<br>2. Explains knowledge base content and prompt design reasoning.<br>3. Includes reflective analysis of design decisions, challenges, and potential improvements. |
| **Presentation and Demonstration** (20 points) | 1. Provides a clear, structured video showcasing the chatbot in action.<br>2. Highlights integration of RAG and ethical guidelines.<br>3. Successfully uploads to personal GitHub repo in the provided format. |

## ⚖ Ethical and Compliance Requirements

- ⚠ **For academic use only; NOT for deployment in clinical settings.**
- Must prominently display a **“Not Medical Diagnosis”** disclaimer in the README.md.
- Must design for crisis detection (e.g., self-harm, violence) and direct users to emergency resources.
- Absolutely no collection or storage of real users’ sensitive personal data.

---

## Recommended Resources

- Ollama Docs
- AnythingLLM Docs
- Prompt Engineering Guide
- OBS Studio (for recording)
- GitHub Documentation (official guide)

---

## Questions / Technical Support

Please email `Yilong.Wu@smu.ca`. Teaching Assistant will respond within 24 hours.

---

*Let's rapidly prototype responsible, domain-aware AI tools that truly support users in healthcare contexts!*