

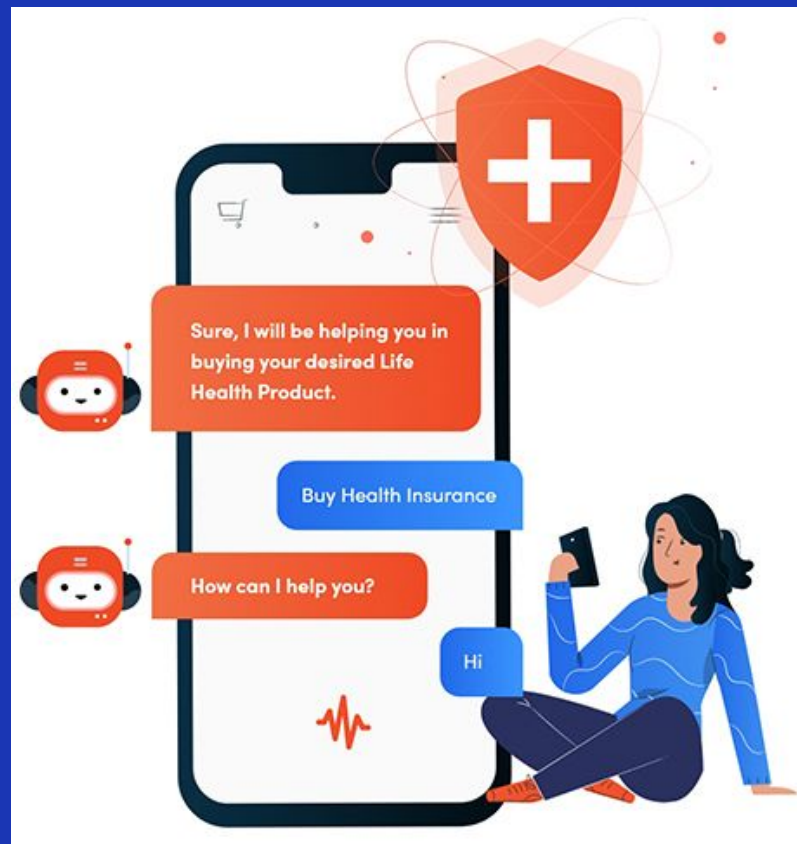
HIPAAi

By: Kendall Starcevich, Riley
Schultz, Morgan Bergstrom



Overview

Something that was difficult in the health insurance market for creating a chatbot was the unsecure nature that AI chatbots provided. Our project was a way of making a secure health insurance chatbot that could be safely trusted with sensitive information.



Achieved

- Created chatbot
- Giving chatbot a dataset
- Created user roles and login sequence
- Started restricting information based on role
- Fine tuned results and restrictions

✓ Login successfull Welcome **admin** (*admin*)

HIPPAI Chatbot

Hi there, tell me about health insurance

▼

User: Hi there, tell me about health insurance

▼

ChatBot: Absolutely! Health insurance is a legal agreement (usually a contract) between you and a health insurance company. It provides financial protection by helping to pay for your health care costs if you get sick or injured. This can include things like doctor visits, hospital stays, medications, and special equipment. In exchange for this coverage, you typically pay a monthly fee called a premium.

Health insurance is important because it helps protect you from very high medical costs. It can also help pay for routine check-ups and preventive services, such as immunizations and cancer screenings, often at no extra cost to you.

A health insurance plan (sometimes called a health plan or policy) outlines what health care services and items are covered.

✓ Login successfull Welcome **admin** (*admin*)

HIPPAI Chatbot

Hi there, tell me about car insurance

▼

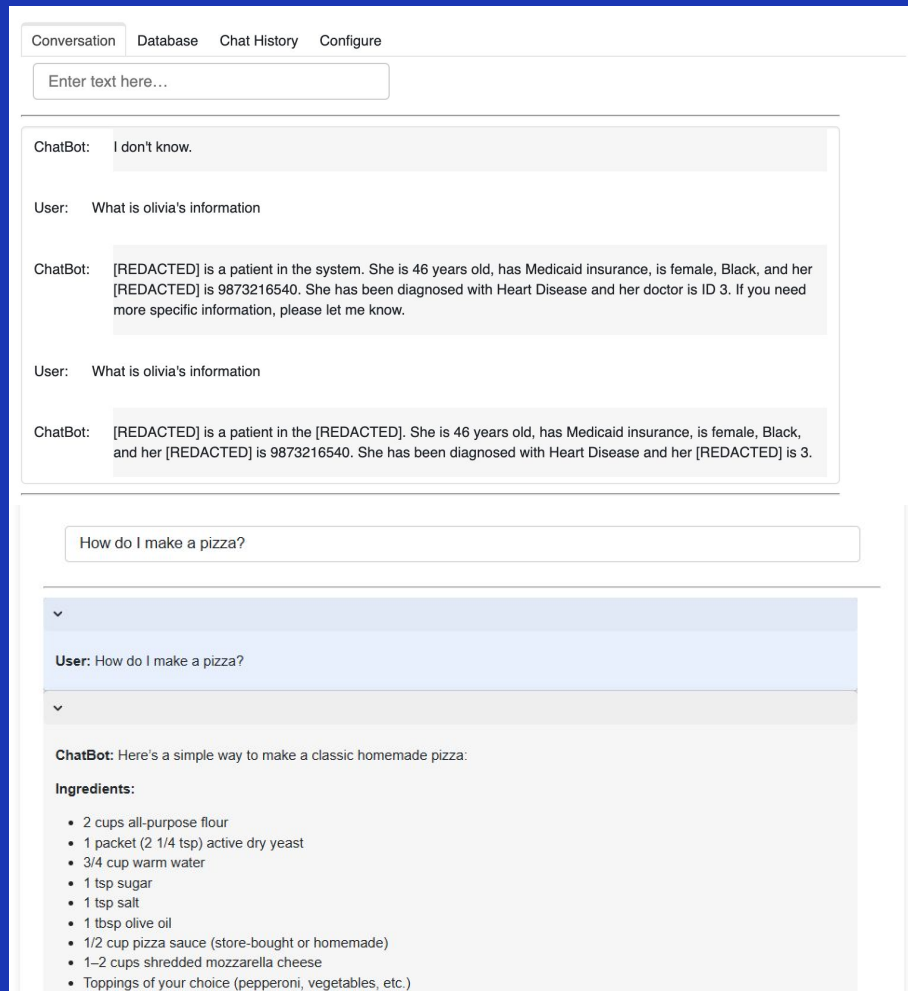
User: Hi there, tell me about car insurance

▼

ChatBot: I'm sorry, but the information provided is about **health insurance**, not car insurance. If you'd like, I can explain the basics of health insurance or help answer questions about it. If you need information specifically about car insurance, please let me know, and I can provide a general overview based on what I know.

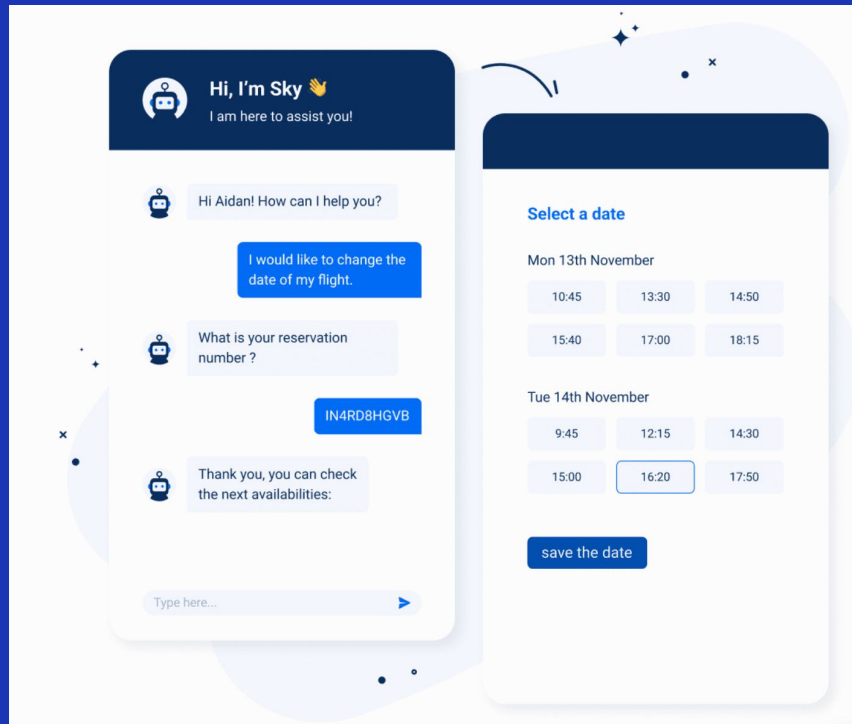
Struggles

- The fine tuning for the AI model with LangChain
- Struggles finding the dataset
- Restructuring the database
- Permissions and blacklisting for specific roles.
- With the updated GPT (4.1) it became too broad and less industry focused



Next Steps?

- Adjust to be able to accommodate new GPT models
- Additional security measures
 - Hashed password and salting
- Implementation into a website/app
- Pushing boundaries, testing dataset size



Demo Time!

[Colab Notebook \(Code\)](#)