Homework: AI Privacy / Anonymization

You’ve been asked by a (private) hospital in the US to put together an LLM-powered chatbot that doctors and nurses can use to quickly retrieve information about patients (of their history, their upcoming medical appointments, etc…). They really prefer using OpenAI directly but are open to other workarounds.

You basically have two options (feel free to share a third or fourth if you have an idea) – you can (1) anonymize sensitive information and then leverage OpenAI / any proprietary model or (2) you can build some open-source on-premise solution.

It is your task to explain to the client their options, and help them make a decision in terms of which way they want to go. Point out the pro and contra elements, how each option affects performance, accuracy, scalability, etc… List and structure all aspects you feel are important to make this decision. Present a very high-level architecture for both options, and for the anonymization version, make sure to mention a couple of concrete solutions (SaaS or custom development).

Present your findings in a deck, do not pay attention to style as content is more important to us. Do not spend more than 12 hours on this task. Don’t forget, no one has the recipe for a perfect LLM-powered chatbot, so all ideas and thoughts are welcome!