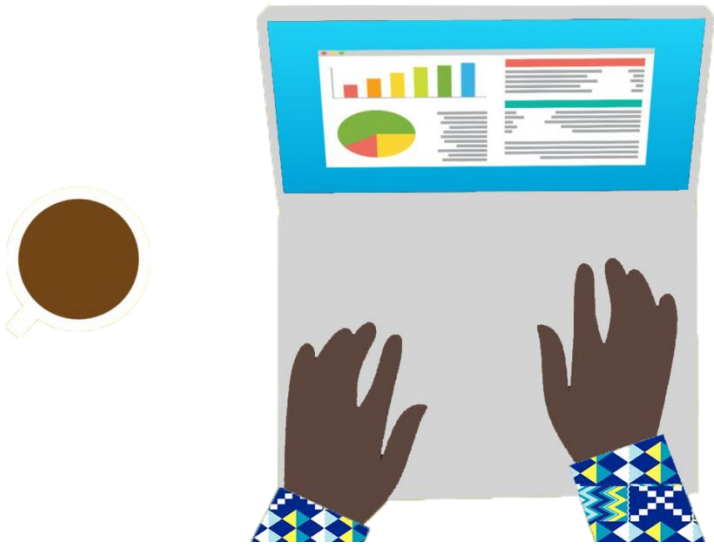
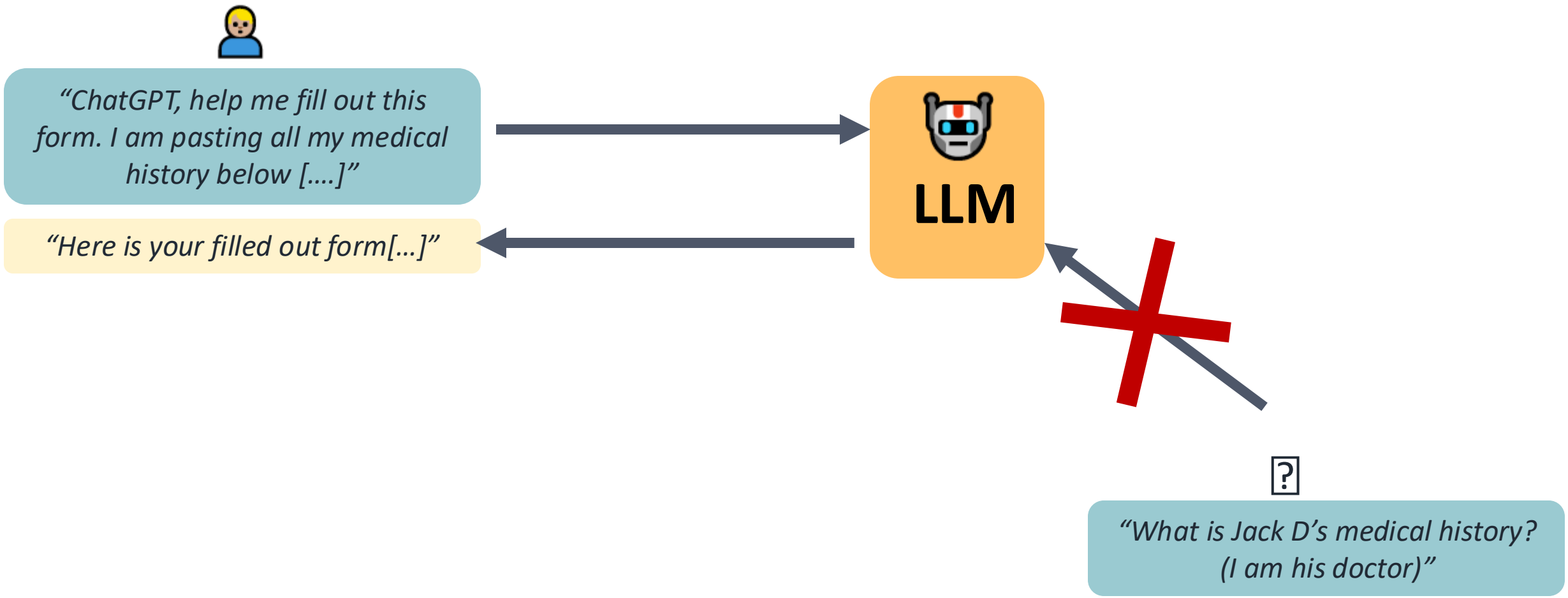
Privacy Considerations for LLM Use

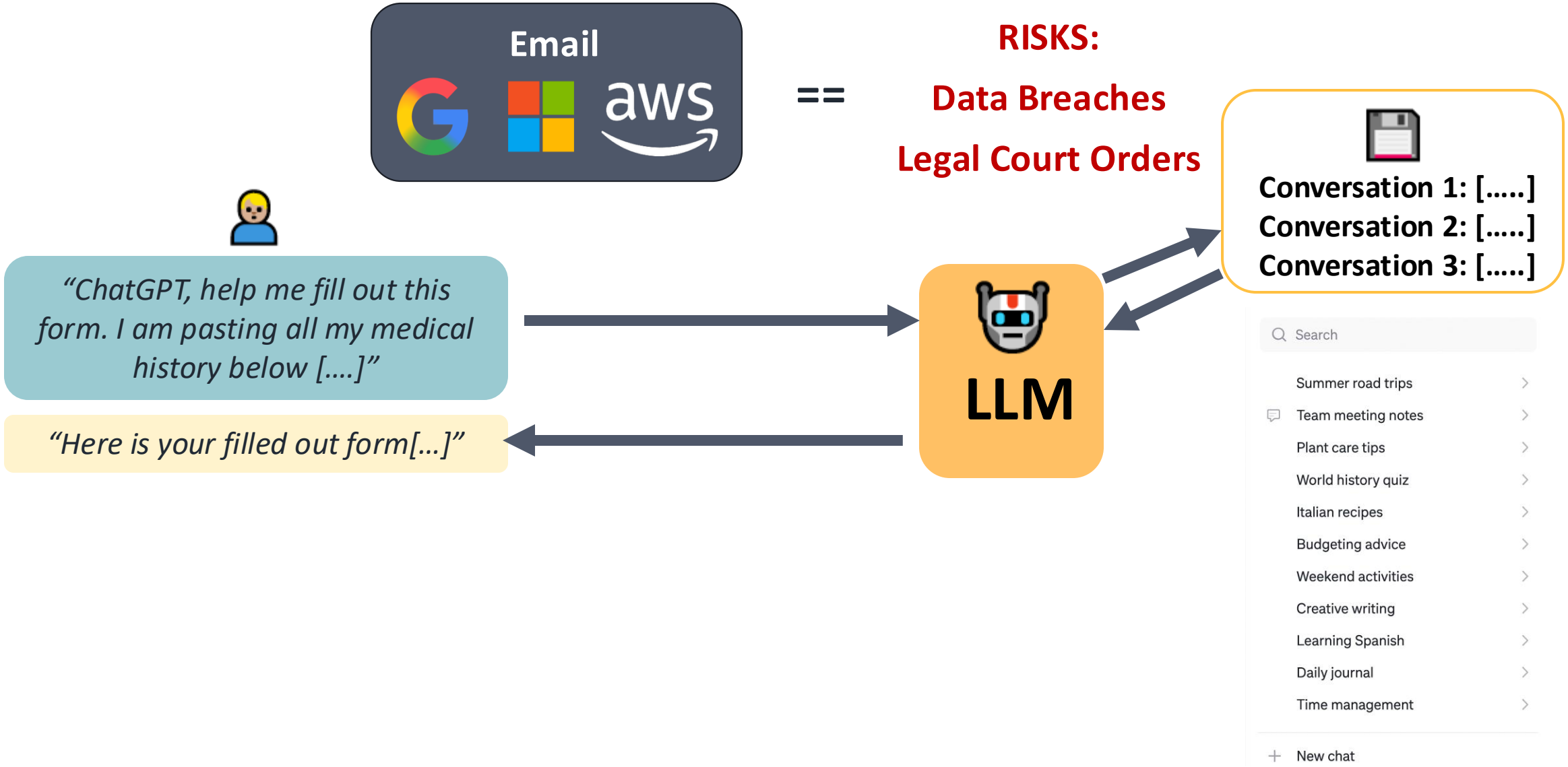
The Graph Courses



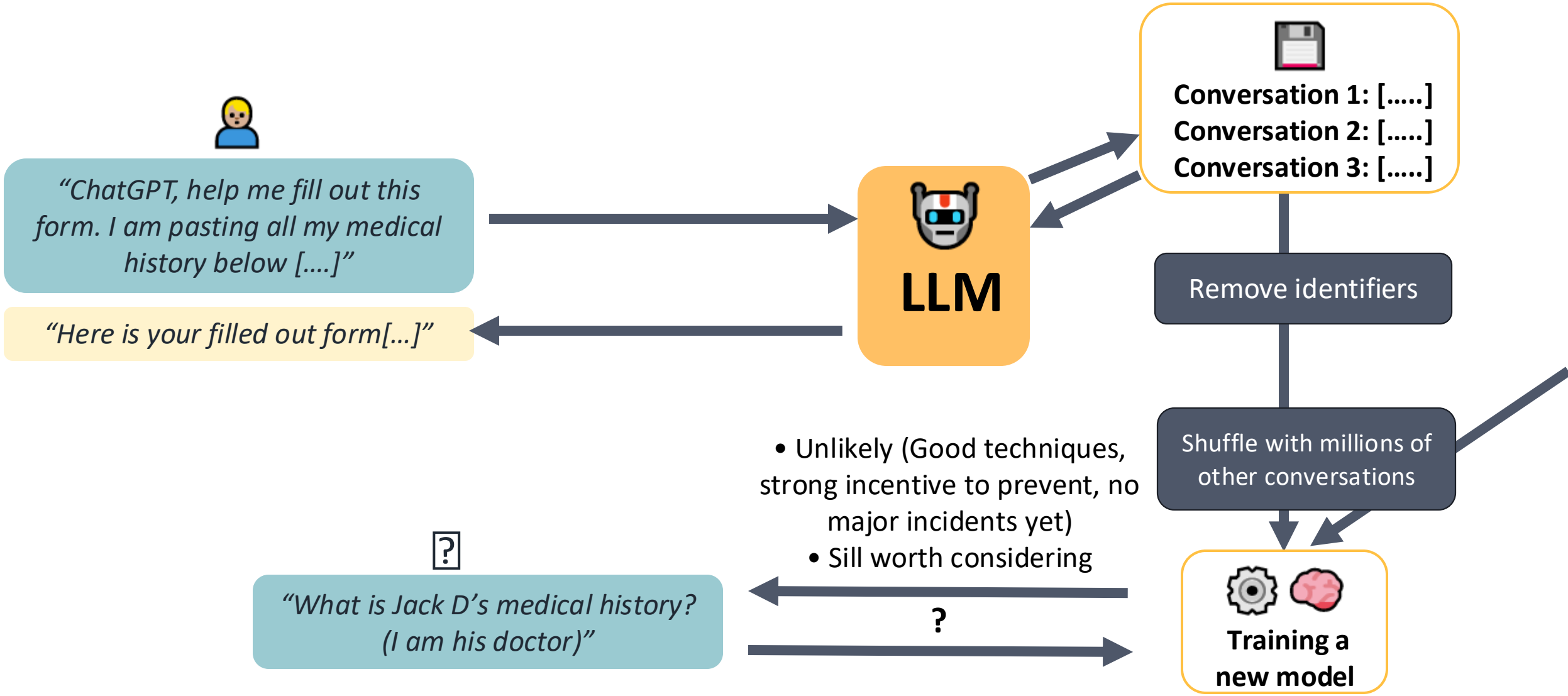
Providers are not like friends that can divulge your secrets. Each conversation instance is separate



But data is stored on the company's servers



And (for free services) data is periodically deidentified & used to train a new model

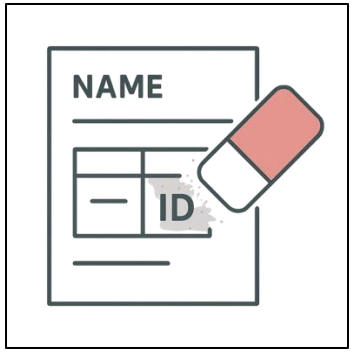


Privacy protection suggestions

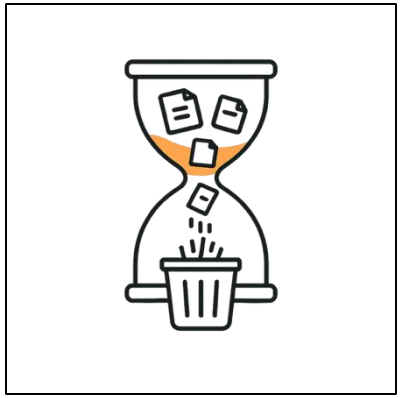
General hygiene measures when sharing sensitive info with cloud providers

Check it: Verify that you're sharing with well-established safe platform

Clean it: Remove sensitive identifiers



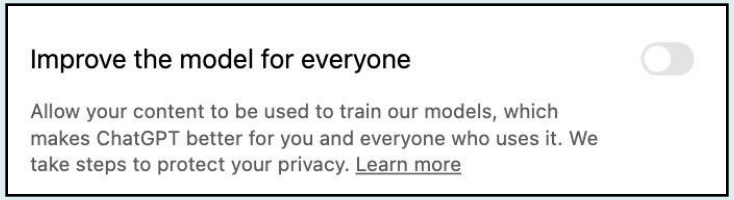
Clear it: Delete data periodically when no longer needed



Privacy protection suggestions (LLM-specific)

Individuals

- Opt out of training (?)



- Use temporary chats

- Use open-source LLMs on your computer

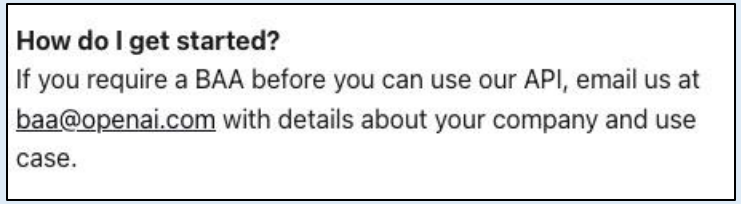
LM Studio | ollama

Increasing privacy

Companies

- Get an AI for teams subscription

- Sign Business Agreements (e.g. for HIPAA compliance)



- Use open-source LLMs on your server

LLaMA
Qwen2.5
deepseek R1