

Privacy Considerations for LLM Use

The Graph Courses





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





"ChatGPT, help me fill out this form. I am pasting all my medical history below [....]"

"Here is your filled out form[...]"



[?]

"What is Jack D's medical history?

(I am his doctor)"

But data is stored on the company's servers





RISKS:

Data Breaches

Legal Court Orders



"ChatGPT, help me fill out this form. I am pasting all my medical history below [....]"

"Here is your filled out form[...]"



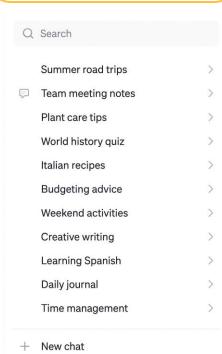
LLM



Conversation 1: [.....]

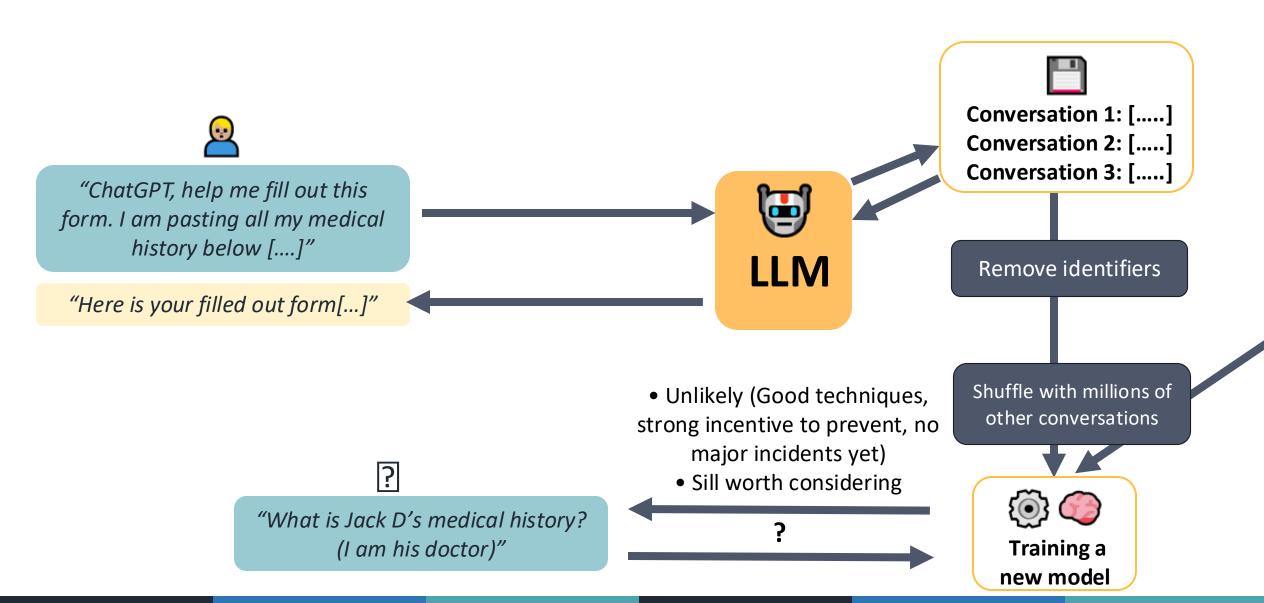
Conversation 2: [.....]

Conversation 3: [.....]



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





Privacy protection suggestions

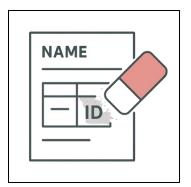


General hygiene measures when sharing sensitive info with cloud providers

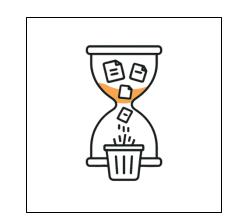
Check it: Verify that you're sharing with well-established safe platform



Clean it: Remove sensitive identifiers



Clear it: Delete data periodically when no longer needed



Privacy protection suggestions (LLM-specific)



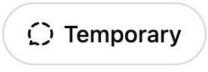


Opt out of training (?)

Improve the model for everyone

Allow your content to be used to train our models, which makes ChatGPT better for you and everyone who uses it. We take steps to protect your privacy. <u>Learn more</u>

Use temporary chats



• Use open-source LLMs on your computer





Increasing privacy



Get an Al for teams subscription



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

How do I get started?

If you require a BAA before you can use our API, email us at baa@openai.com with details about your company and use case.

• Use open-source LLMs on your server

