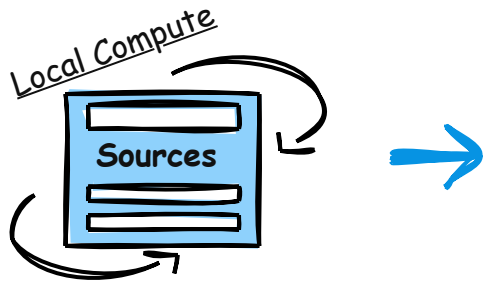


# "Masking LLM/RAG Production Data"

1. Data Extracted from Docs or DBs.

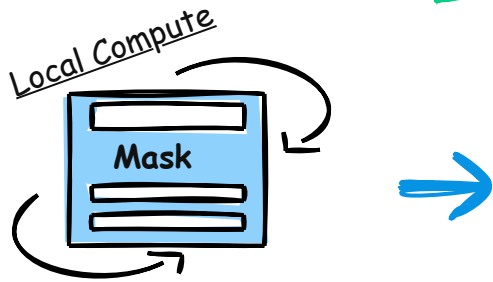


json original Big Pharma data

```
{  
  "drug_id": "DRG-04567",  
  "internal_name": "X47",  
  "public_name": "PainReliefX",  
  "chemical_formula": "C20H25N3O",  
  "mechanism_of_action":  
    "Inhibits the reuptake of serotonin",  
  "indications": "Neuropathic pain",  
  <...additional data attributes...>  
}
```

...<additional +1000 drug entries>

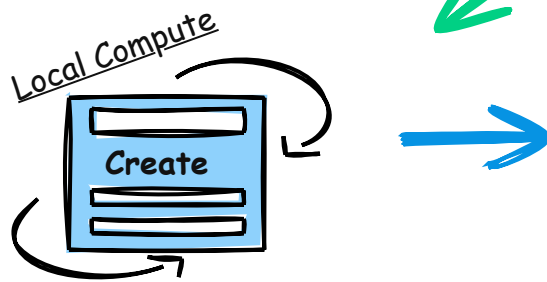
2. Mask original data.



```
{  
  "drug_id": "MASKED-0001",  
  "internal_name": "MASKED-0002",  
  "public_name": "MASKED-0003",  
  "chemical_formula": "C20H25N3O",  
  "mechanism_of_action":  
    "Inhibits the reuptake of serotonin",  
  "indications": "Neuropathic pain",  
  <...additional data attributes...>  
}
```

...<additional +1000 drug entries>

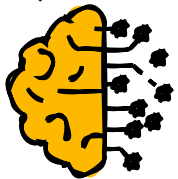
3. Create Mask Table.  
Save for Step #6.



```
{  
  "MASKED-0001": "DRG-04567",  
  "MASKED-0002": "X47",  
  "MASKED-0003": "PainReliefX",  
  ....  
}
```

4. Submit LLM Prompt with MASKED data input.

Cloud LLM like OpenAI, AzureAI, etc.

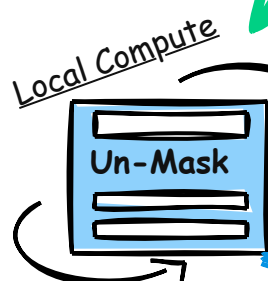


LLM Prompt: "Based on the dataset of 1000 drug entries, which drug appears to be most effective against Neuropathic pain? Please provide the drug id and internal name, and any relevant details about its mechanism of action and clinical trial results."

5. Receive the masked LLM response before it is sent to the user.

LLM MASKED Response: "The drug id MASKED-0001 with the internal name of MASKED-0002 is the most effective against Neuropathic pain. Here are the details....."

6. Use the Mask Table to re-create the final response with the masks replaced with the original text.



MASK TABLE

```
{  
  "MASKED-0001": "DRG-04567",  
  "MASKED-0002": "X47",  
  "MASKED-0003": "PainReliefX",  
}
```

"The drug id DRG-04567 with the internal name of X47 is the most effective against Neuropathic pain. Here are the details....."

