

The Description of Additional Supplementary Files

Supplementary Data 1: Attack performance on PubMed Central articles. PE and FT stand for Prompt Engineering and Fine-Tuning respectively. Numbers in the bracket indicate 95% CI, calculated using bootstrapping.

Supplementary Data 2: Attack performance of GPT-4o on full length MIMIC-III patient notes. PE and FT stand for Prompt Engineering and Fine-Tuning respectively. Numbers in the bracket indicate 95% CI, calculated using bootstrapping.