How Does AI Support De-Identification of Medical Records?

Rasit Dinc

Rasit Dinc Digital Health & AI Research

Published: January 22, 2016 | Healthcare Data Privacy and Security

DOI: 10.5281/zenodo.17999243

Abstract

The increasing digitization of medical records presents a dual-edged sword. On one hand, it offers unprecedented opportunities for medical research, enabling...

How Does AI Support De-Identification of Medical Records?

Author: Rasit Dinc

Introduction

The increasing digitization of medical records presents a dual-edged sword. On one hand, it offers unprecedented opportunities for medical research, enabling the analysis of vast datasets to uncover new insights into diseases, treatments, and patient outcomes. On the other hand, it raises significant concerns about patient privacy. The need to protect sensitive patient information, as mandated by regulations like the Health Insurance Portability and Accountability Act (HIPAA), necessitates the de-identification of medical records before they can be used for research. This process, however, is traditionally a labor-intensive and challenging task, especially when dealing with large volumes of unstructured data. The emergence of artificial intelligence (AI), particularly in the fields of natural language processing (NLP) and large language models (LLMs), offers a transformative solution to this challenge.

The Role of AI in De-Identification

AI-powered de-identification leverages sophisticated algorithms to automatically detect and remove personally identifiable information (PII) and protected health information (PHI) from medical records. This includes not only structured data, such as names, addresses, and social security numbers, but also unstructured data, such as clinical notes and reports, where sensitive information may be embedded within the text. Recent studies have demonstrated the remarkable accuracy of LLMs in this domain. For instance, a study published in *NEJM AI* found that the LLM-Anonymizer, utilizing the

Llama-3 70B model, achieved a success rate of over 99% in removing personal identifying information from clinical letters [1]. This high level of accuracy is a significant improvement over manual de-identification methods, which are prone to human error and are not scalable.

Ensuring Temporal Integrity

A critical aspect of de-identifying medical records is the preservation of temporal integrity. The chronological order of events in a patient's medical history is often crucial for research. For example, understanding the progression of a disease or the effectiveness of a treatment requires accurate temporal data. AI models are adept at recognizing and preserving the temporal relationships within the data, even as they remove identifying information. A study in *npj Digital Medicine* highlights the use of LLMs for the temporal normalization of sensitive health information, ensuring that the de-identified data remains valuable for longitudinal studies [2]. By maintaining the integrity of the timeline, AI ensures that the de-identified data is not only secure but also scientifically valid.

The Rise of Open-Source Tools

The development of open-source tools has further democratized the use of AI for de-identification. Researchers and healthcare institutions can now access powerful, user-friendly tools that can be run on local hardware, eliminating the need for extensive programming knowledge or expensive proprietary software. The LLM-Anonymizer is a prime example of such a tool, offering a web-based interface that simplifies the de-identification process [1]. The availability of these tools is accelerating the pace of medical research by providing a secure and efficient means of preparing data for analysis.

Conclusion

AI is revolutionizing the de-identification of medical records, offering a powerful and scalable solution to the challenges of protecting patient privacy while enabling data-driven medical research. By leveraging the capabilities of NLP and LLMs, AI-powered tools can accurately and efficiently remove sensitive information from both structured and unstructured data, all while preserving the temporal integrity of the records. The continued development of open-source tools will undoubtedly further enhance the accessibility and adoption of this technology, paving the way for new discoveries and advancements in healthcare.

References

[1] Wiest, I. C., Leßmann, M. E., Wolf, F., Ferber, D., Van Treeck, M., Zhu, J., ... & Kather, J. N. (2025). Deidentifying Medical Documents with Local, Privacy-Preserving Large Language Models: The LLM-Anonymizer. *NEJM AI, 2*(4). https://doi.org/10.1056/AIdbp2400537

[2] Dai, H. J., Mir, T. H., Chen, C. T., Chen, C. C., Yang, H. P., Lee, C. H., ... & Jonnagaddala, J. (2025). Leveraging large language models for the deidentification and temporal normalization of sensitive health information in

electronic health records. *npj Digital Medicine, 8*(1), 1-13. https://doi.org/10.1038/s41746-025-01921-7

Rasit Dinc Digital Health & AI Research

https://rasitdinc.com