UW Medicine Interim Guidance for Generative AI in the Healthcare Setting

February 16, 2024

UW Medicine is in the process of developing a comprehensive institutional approach to the responsible use of generative artificial intelligence (commonly referred to as generative AI), including large language models (LLMs), in the healthcare setting. We appreciate your patience as we take a thoughtful approach to this evolving space, which balances both the opportunities and risks these tools present for healthcare organizations. The purpose of this document is to provide interim guidance on how generative AI, including LLMs (e.g., ChatGPT, ambient listening tools), may or may not be used at UW Medicine.

If you have a question that is not addressed in this interim guidance, please direct your inquiry to the email address we have established to intake questions and other feedback: GenAIatUWM@uw.edu.

1. **What are generative AI and large language models (LLMs)?**

   Artificial Intelligence (AI) is a term used to refer to a broad variety of computational systems that perform tasks thought to require human intelligence. LLMs, or Large Language Models, are advanced artificial intelligence systems that have been trained on large and expanding amounts of text data to generate human-like language patterns. With specialized training, LLMs can interpret context in a wide range of tasks, such as translation, summarization and conversation. Consequently, contemporary LLMs have an unprecedented ability to follow instructions provided in natural language.

   Generative AI refers to a class of artificial intelligence models, like LLMs, that have the capability to generate new content, such as text, images, or even audio and video, that is coherent and contextually relevant based on the patterns learned from their training data. In the case of LLMs, the language generated generally appears fluent and has plausible content, though it is not always factually accurate.

2. Where might you see this functionality?

Generative AI, including LLMs, can take a variety of forms. For example:

- Publicly available generative AI (e.g., DALL-E) and LLMs (e.g., OpenAI's ChatGPT)
- Generative AI, including LLMs, in research and development (both those developed at UW Medicine or externally)
- Generative AI, including LLMs, that provide additional functionality to an existing tool we use (e.g., new functionality within Epic and Microsoft Office products)
- Generative AI, including LLMs, that are, or are part of, a new product or service being offered to UW Medicine

3. How is UW Medicine addressing generative AI and LLM tools and their potential use in the healthcare setting?

In August 2023, Dr. Tim Dellit, UW Medicine's Chief Executive Officer and Dean for the UW School of Medicine, charged an interdisciplinary workgroup to gather information and provide a foundation to develop an institutional approach for the responsible use of generative AI, including LLMs. This group's purpose was to ensure UW Medicine is prepared to address the unique considerations these tools raise in the healthcare setting, including patient care, business operations supporting our healthcare activities (e.g., revenue cycle, human resources, supply chain) and research integrated with the clinical environment. For purposes of this work, "research integrated with the clinical environment" includes: 1) when our clinical data, including de-identified patient data, is used to prompt, test, train or fine-tune generative AI, including LLMs; and 2) clinical trials (or other clinical research studies) involving generative AI, including LLMs.

Specifically, the group was charged with:

- Recommending guiding principles for the responsible use and training/fine-tuning of generative AI, including LLMs;

- Surveying existing and potential applications that UW Medicine might contemplate using;
- Providing an overview of the legal, regulatory, ethical and mission-related risks associated with these tools in the healthcare setting;
- Recommending a committee or governance structure for developing policies, addressing issues and overseeing UW Medicine's institutional approach; and
- Setting forth, at a high-level, policies, processes, awareness and education, resources, physical and IT infrastructure, privacy and security measures, investment, communication, etc. that may be needed over time for UW Medicine to successfully navigate increasing use of these tools in the healthcare environment.

4. **When will this work be complete?**

   The workgroup submitted its high-level recommendations to Dr. Dellit on January 31, 2024. The workgroup's final report can be accessed here: https://huddle.uwmedicine.org/wp-content/uploads/2024/02/LLM-Workgroup-Preliminary-Report.pdf.

   In approving the recommendations, Dr. Dellit charged a UW Medicine Generative AI Task Force with building upon the work of the LLM Workgroup and developing the business plan and infrastructure needed to support a permanent, steady-state approach to use of generative AI in the healthcare setting. If you have questions regarding the Task Force, please reach out to Ana Anderson, Senior Director of Business Affairs for UW Medicine, who is chairing the Task Force (aanders@uw.edu).

5. **Can I use a publicly available generative AI or LLMs (e.g., OpenAI's ChatGPT, Google's BARD/Gemini, or others) to assist me in my job?**

   Yes, with the following limitations:
   i) Users must not share (e.g., manually entered, via APIs, etc.) any of the following data with these tools:

- UW Medicine patient data or clinical data of any kind, including de-identified patient data
- Personally identifiable information
- Proprietary UW Medicine data
- Intellectual property of any kind

ii) Users must not:

- Use information derived from the tools to inform clinical care
- Rely on information derived from the tools without validation
- Disseminate content generated by the tools without careful review
- Utilize programming code from an external LLM without code undergoing additional security review as described below
- Leverage the tools for automating workflow

6. **What if I am already using a generative AI tool in a manner that is inconsistent with the guidance in this document?**

   Please discontinue use immediately. Reach out to GenAIatUWM@uw.edu to get connected with a team member who can partner with you for additional discussion.

7. **Are any generative AI tools specifically prohibited?**

   UW-IT and UW Medicine ITS have prevented the use of certain tools on Zoom and Microsoft Teams. For example, Read.AI, which is a tool that generates meeting notes, cannot be used.

Clinical Care & Healthcare Operations

This guidance applies to use of generative AI, including LLMs, for patient care or other business supporting the healthcare enterprise.

8. **Can I put UW Medicine clinical data (whether identifiable or not) into a generative AI or LLM tool to support my work?**

   No.

9. **Are there any generative AI or LLM tools that UW Medicine has approved for clinical use in the healthcare setting (separate from research)?**

   Not yet. We are evaluating Epic functionality that would create draft responses to patient inquiries through MyChart for providers to review and edit before sending to the patient. A multi-disciplinary group is assessing whether (and if so, how) to implement this functionality.

   Use of tools such as Freed.AI for ambient note generation during a clinical visit or internally developed tools deployed for clinical use **cannot** be utilized at this time. If you are uncertain whether a particular tool can be used, please direct your inquiry to: GenAIatUWM@uw.edu.

10. **I am interested in using a generative AI or LLM tool that would have access to UW Medicine clinical data (either one developed in-house or from a third-party). Who should I work with?**

    UW Medicine is in the process of developing an infrastructure (including policy and operational processes) and governance approach to the use of generative AI, including LLMs, in the healthcare setting.

    Until this structure is formalized, we have established an interim intake and review process. You can submit your inquiry to GenAIatUWM@uw.edu and a team member will reach out to you.

11. **I'm not sure if the tool/functionality I am exploring or functionality that is being added by a third-party to an existing approved tool qualifies as generative AI, an LLM or a predictive analytics tool. Who can help me?**

    Please send any such inquiries to GenAIatUWM@uw.edu.

Research

This guidance applies to research involving generative AI, including LLMs, that is integrated with the clinical environment.

12. When is research "integrated with the clinical environment"?

- When using clinical data, including de-identified patient data, to prompt, test, train or fine-tune generative AI, including LLMs
- When conducting a clinical trial (or other clinical research study) involving generative AI, including LLMs

13. Are there any unique requirements for conducting this type of research?

This type of research must undergo a security risk review by UW Medicine. If an applicable study requires IRB approval, the UW IRB application form will prompt researchers to obtain the security review. Even if IRB approval is not required, projects involving use of generative AI, including LLMs, with de-identified data **must** undergo a security risk review. You can initiate a swift security risk assessment by completing the Honest Broker Intake Form.

The security risk review is necessary to ensure the protection of sensitive data, maintain compliance with privacy regulations and mitigate potential risks associated with the use of generative AI, including LLMs. Additionally, it helps identify and address security vulnerabilities and safeguards the confidentiality and integrity of the data being processed by these advanced AI technologies.

14. What about research that is *not* integrated with the clinical environment?

This interim guidance does not address research that is not integrated with the clinical environment. However, we encourage careful review of terms of use before using generative AI, including LLMs, for research, especially when using them on unpublished work product, ideas or data. Additionally, terms should be reviewed prior to submitting any data, ideas or work product generated using state or federal funds.