**AI IN MEDICINE**

The Challenges for Regulating Medical Use of ChatGPT and Other Large Language Models

The introduction of artificial intelligence (AI) into medical devices, decision support, and clinical practice is not new, with a particular uptick in investment and deployment within the past decade. Regulators (eg, the US Food and Drug Administration, the European Medicines Agency, and the National Medical Products Administration), intergovernmental organizations (eg, the World Health Organization), civil society groups, institutional review boards at hospitals, and others have worked hard to define the scope of what AI applications should require review and approval, implementing rules in a fast-changing terrain with mixed results.

What has changed is the public availability and interest in large language models (LLMs), most notably OpenAI’s ChatGPT and Google’s Bard, with potential applications in medicine. These LLMs are large (1 trillion parameters for GPT-4 and growing), general rather than trained for a specific task (though fine-tuning is possible), autoregressive (using only past data to predict future data), and foundational (likely to be the seed for many further devices and applications). There has also been interest in creating LLMs with more curated medical training data, such as Google’s Med-PaLM 2.

Regulating all of these selected areas is delicate and only a starting point because new risks and benefits will emerge as LLMs evolve and become more prominent for medical uses.

The medical world has taken note, with a wide range of uses from generating draft progress plans to answering patient questions via a chatbot. In this Viewpoint, we discuss how regulators across the world should approach the legal and ethical challenges raised by medical use of LLMs, including privacy, device regulation, competition, intellectual property rights, cybersecurity, and liability.

**Privacy**

Large language models are trained on vast amounts of data scraped from the web and other digital sources, which may contain personal data. In the European Union, the General Data Protection Regulation only permits access to personal data, including health data, when there are specific justifications (eg, informed consent or public interest). OpenAI’s ChatGPT is currently under investigation by European authorities to assess compliance with the General Data Protection Regulation. A different privacy problem may occur in the US under the Health Insurance Portability and Accountability Act of 1996 or under privacy laws for individual states if physicians include protected patient data in prompts they submit to LLMs.

The more general ethical questions that regulators need to grapple with are: When is the scraping of patient data from the web or other data sets permissible? Should patients be able to opt out of such data uses? An important first step would be for privacy regulators in the US, the European Union, and elsewhere to issue specific guidance, binding or advisory, as to privacy permissible and impermissible ways to develop and deploy LLMs. Harmonization between these regulators is also an important next step to the extent possible.

**Device Regulation**

Under laws in the US and the European Union, LLM software that is only developed for general purposes and without any claims to their use for medical purposes would usually not qualify as medical devices. However, LLMs that are developed, modified, or directed toward specific medical purposes, such as through interaction with medical devices or by helping clinicians reach medical decisions and communicating with patients, might be treated as medical devices.

Policing the line of intended use will be tricky. There may also be particular concerns about open-source LLMs that may be regarded as so-called software of unknown provenance if a third party adapts or uses them as a component in a medical device, which would trigger special compliance standards and require sufficient documentation that may not always be accessible. Device regulators need to clarify when incorporating an LLM into a medical product renders it a medical device under existing regulations, make fundamental decisions about how to manage adaptive learning in LLMs, and consider how existing risk classification approaches apply to the distinctive setting of LLM use in devices.

**Competition Law**

Now, at the dawn of medical use of LLMs, one could envision 2 very different futures. One future is a vibrant ecosystem of medical LLMs trained on different data sources with very different designs; the other future is one where 2 or 3 large corporations dominate the LLM market and license their products to all medical users. Each future poses real trade-offs. Can a large number of small...
companies adequately ensure privacy and other ethics by design? Will consumers be able to adequately distinguish high- and low-quality LLMs in a crowded market? Will the dominance of a small number of LLM developers result in model homogeneity? Would a small number of developers exert market power in a way that increases prices for patients and health care systems? Antitrust regulators have a key role to play in determining where the world ends up in between these 2 very different futures. Moreover, the requirements set by medical regulators for market entry and the flexibility level of medical regulations will also have a huge effect on the competitive landscape.

**Intellectual Property**

The competition policy analysis in turn depends on what intellectual property rights are recognized in LLMs. Recognizing too many intellectual property rights at the computing, data creation, and foundation modeling stages of LLM development could create increased barriers to entering the market. Recognizing too few intellectual property rights, though, may deter some market entrants because they may be unable to raise enough capital based on claims of having an exclusive product at the end of development. The fact that LLMs are often trained on enormous amounts of opaque data sources raises the specter that they themselves may violate existing intellectual property rights. This concern and the lack of transparency for current LLMs recently resulted in changes to the proposed Artificial Intelligence Act in the European Union, and now requires companies deploying generative AI tools to disclose any copyrighted material used to develop their systems.

**Cybersecurity and Liability**

Large language models may be a force for good or evil for medical cybersecurity. Generative AI can play a key role in scanning digital logs, finding patterns in vulnerability exploitation, and helping clinicians improve cybersecurity systems. But security vulnerabilities of LLMs can allow their manipulation and turn them into misinformation sources, generators of more sophisticated and automated fraudulent attacks, or spreaders of malware. Hence, minimum security thresholds should be set before rolling out LLM applications in health care and drug development settings.

For example, foundational open-source AI tools should be based on a programmatic core that effectively reduces the risk of hacks and manipulation. Regulators must also ensure that physicians and other medical staff are well trained on how LLMs work, their limitations, and cybersecurity risks. Lawmakers must consider whether they have adequate structures to hold developers accountable and liable for noncompliance with such standards. It will also be important to clarify when developers can lawfully require that users waive liability claims or indemnify developers from future harms as OpenAI, for example, purports to do at the moment.

Regulating all of these selected areas is delicate and only a starting point because new risks and benefits will emerge as LLMs evolve and become more prominent for medical uses. The challenge is not just in the governance of these technologies but in limiting to the current mechanisms of governance. One governance approach is to try to prohibit the use of LLMs in certain spheres. Within the last several months, some countries have announced that they would do so, but most have backed off given the changes that have been made by developers. We are skeptical whether this will be feasible in the long term both because of political pressure and the ability to circumvent such restrictions. Moreover, the recently introduced changes to the proposed Artificial Intelligence Act in the European Union (in response to the recent LLM developments) demonstrates that overly detailed and rigid legislation will face severe update challenges with regard to new technological developments.

Meanwhile, voices in industry are urging governments to hold off on regulating in favor of allowing self-regulation by the LLM industry. A different approach is to try to pass new legislation focused on LLMs. The proposed Artificial Intelligence Act in the European Union could serve as a model. The problem is that such legislation risks rigidly bonding medical AI to today’s technical standards, which may be inadequate for tomorrow’s problems. We believe that these forms of governance will be important, but so is more open-ended delegation of authority to regulate medical AI to administrative agencies like the US Food and Drug Administration and the European Medicines Agency as well as common law decision-making by courts, especially regarding liability questions.

---

**ARTICLE INFORMATION**

Published Online: July 6, 2023. doi:10.1001/jama.2023.9651

Conflict of Interest Disclosures: Dr Minssen reported receiving grants from the European Union; serving as a consultant to Corti; and serving on advisory boards for Christian Hansen Holding A/S and the World Health Organization. Dr Vayena reported serving on ethics advisory panels for IQVIA, Merck KGaA, and the World Health Organization. Mr Cohen reported serving on ethics advisory boards for Illumina and Bayer.

Funding/Support: Dr Minssen and Mr Cohen reported receiving grants from the European Union. Mr Cohen reported serving on ethics advisory panels for Christian Hansen Holding A/S and the World Health Organization. Dr Vayena reported serving on ethics advisory panels for IQVIA, Merck KGaA, and the World Health Organization. Mr Cohen reported serving on ethics advisory boards for Illumina and Bayer.

Role of the Funder/Sponsor: The Novo Nordisk Foundation had no role in the preparation, review, or approval of the manuscript or decision to submit the manuscript for publication.

**REFERENCES**