

Daily Journal

MAY 22, 2024

TOP INTELLECTUAL PROPERTY LAWYERS

2024

COLUMN

IP issues of artificial intelligence in health care: From the “original sin” to the prospect of mandated transparency

BY RODERICK "ROD" M. THOMPSON AND
RODERICK "RORY" MACKENZIE THOMPSON

Artificial intelligence (AI) has the potential to revolutionize health care by automating tasks, assisting with complex processes and augmenting human capabilities. The use of AI in medicine is not new. The Food and Drug Administration (FDA) has approved more than 650 AI-enabled medical devices since 1995. The medical device regulatory framework, however, is limited in its ability to evaluate next-generation AI technologies. To date, there have not been any FDA-approved devices that employ generative AI or artificial general intelligence, or are powered by large language models (LLMs). The dynamic nature and flexible uses of such software may be incompatible with the FDA's emphasis on standardized trials to evaluate medical device performance.

Meanwhile, generative AI is being rapidly deployed in other, less regulated areas of health care, such as administrative applications, clinical enterprise tools and patient-facing wellness apps. In response, policymakers appear headed toward a

regulatory approach focused on increasing transparency, equipping users with the information necessary to make informed choices about using AI in health care. This regulatory focus, coupled with the ever-increasing use of personal and copyrighted information in many health AI applications, reinforces the primacy of data and the importance of IP in health care AI.

FAIR USE AND THE “ORIGINAL SIN”

The use of AI in health care raises the same intriguing and so far unresolved copyright issues common to other fields. According to a recent investigation by the New York Times, OpenAI and other creators of generative AI engines allegedly scraped all available English language text content on the internet for training and “ran out of data” by late 2021. (“A.I.’s Original Sin,” “The Daily”podcast, April 16, 2024, Tr. 3:23-48.) Not coincidentally, these same players are on opposite sides in a copyright lawsuit pending in the South-



Roderick "Rory" Mackenzie Thompson, M.D., M.Sc., is internal medicine physician and Policy Fellow with the Stanford Byers Center for Biodesign.



Roderick "Rod" M. Thompson is a JAMS arbitrator, mediator and neutral evaluator based in the San Francisco Resolution Center. He has extensive experience as both a trial lawyer and a neutral in resolving disputes involving technology, intellectual property, and competition issues.

ern District of New York: *New York Times v. Microsoft Corp., OpenAI, et al.*, Case No.: 23-11195, filed Dec. 27, 2023. New

Your Times is one of the dozens of pending cases raising the issue of whether the use of scraped copyrighted material

for training generative AI is a protected fair use under the Copyright Act and the recent Supreme Court precedents in *Warhol Foundation v. Goldsmith* and *Oracle v. Google*.

In addition to fair use, some of these pending cases raise the training issue in the context of protected patient data. For example, the complaint in *A.T., J.H., v. Open AI LP, et al.* (ND Cal. filed 9/5/2023), Case No.: 3:23-cv-04557-VC, brought by a class of software engineers alleges that AI products store the personal information of their users, including “private health information obtained through the management of patient portals such as MyChart” and their training data contains information about “our mental health and ailments.” (16 and 74.)

The unauthorized use of such confidential patient data is a significant concern to patients and medical professionals alike.

RISK OF ACCESS TO CONFIDENTIAL PATIENT DATA

Confidentiality, or lack thereof, is a core concern for generative AI models. Lawyers are warned never to input any confidential information of the client into any generative AI model without anonymizing it. Similarly, health

care systems routinely warn their employees not to use LLMs for clinical purposes because any information inputted can be saved and integrated into the model. These warnings do not address the risk of patients unwittingly revealing their personal health information (PHI) by using consumer health AI applications.

LLMs can rapidly integrate user preferences and continuously refine communication approaches to individual users. Such powerful communication tools have the potential to drive patient engagement and positive behavior changes. However, the same technology that can be harnessed to help people lose weight or take their medications correctly can also be used to manipulate consumers to disclose their PHI or follow dangerous medical advice. Unlike communications with health care professionals through secure portals, most AI consumer health apps are not subject to HIPAA protections. Personal data has become the real currency of the internet. Consumers may not be aware of how their personal data is collected and used. Fine-print disclosures buried in user agreements do not adequately warn that when using the internet, you are the product.

THE PROTECTIONS AFFORDED BY AND RISKS OF GREATER TRANSPARENCY

Government regulation of AI is in its infancy. Approaches by state and federal government agencies are evolving. The EU seems headed for more prescriptive government edicts than the United States. One common theme running through many proposals is the requirement of disclosures to promote transparency. Last month, U.S. Rep. Adam Schiff proposed the Generative AI Copyright Disclosure Act, which would require anyone creating or changing a training dataset for a generative AI system to file with the Copyright Office a summary of all copyrighted works used. The disclosure requirement would apply retroactively when already-released systems are changed.

In the health care space, the Office of the National Coordinator for Health Information Technology, which creates standards for health care IT systems such as electronic health records, released a final rule in December 2023 that specifies new transparency and risk-management requirements for developers using AI. HTI-1 requires software developers to disclose certain “source attributes” of AI algorithms to users. Developers have raised concerns that given dif-

ficulties obtaining copyright and patent protections for software, extensive disclosure requirements for AI algorithms may expose developer intellectual property to exploitation by competitors. There is an unavoidable tension between the interest of users in necessary transparency about the training and function of health AI models and the interest of developers to maintain confidentiality.

The challenges posed by AI are magnified by the importance society places on patients’ control over their PHI and their agency to make informed health care decisions. The American Medical Association prefers the term “augmented intelligence” rather than “artificial intelligence” to emphasize the primacy of humans in the decision-making process and the desired limitation of automated systems to a role of only “augmenting” human function. Changing AI’s name will not lessen the insatiable appetite of AI systems for huge volumes of data nor business interests in protecting IP and keeping trade secrets confidential.

Disclaimer: This content is intended for general informational purposes only and should not be construed as legal advice. If you require legal or professional advice, please contact an attorney.