DAY PITNEY LLP

www.daypitney.com

Generative AI in Healthcare: Diagnosing the Legal Landscape for Dr. GenAI

By Kritika Bharadwaj and Colton J. Kopcik, Day Pitney LLP

Artificial Intelligence (AI) technology, encompassing machine learning and deep learning models, operates through algorithms that enable systems to automatically learn from historical data and make predictions or decisions. This technology is not new to healthcare. It has now evolved into a more revolutionary form of AI, generative artificial intelligence (GenAI). GenAI algorithms learn from vast datasets to generate synthetic data or new content in a variety of formats. GenAI, especially those relying on the Large Language Models (LLMs) such as GPT-4 that was introduced in March 2023, employs a technique called tokenization for natural language processing (NLP) of data, whereby sequences of tokens are analyzed instead of entire sentences or paragraphs. This allows the LLMs to efficiently train on and analyze massive volumes of data to generate human-like text.

This recent development suggests that GenAI may be applied in various healthcare sectors, including diagnostics, treatment planning, medical research, and education. The digitization of clinical notes, medical imaging and records in conjunction with the need to effectively utilize such data in the provision of medical services, may prove to be the “pre-op” for NLP of such electronic data by LLMs in the near future.

While AI-based medical technologies based on other deep learning methods are already applied in healthcare services, and also regulated under healthcare laws (for example, AI and machine learning (ML) based medical devices are regulated by the FDA), the utilization of medical data by GenAI models to train LLMs for content generation is not explicitly contemplated in current healthcare regulations.

The potential of GenAI, particularly in the context of its use of protected health data, has caught the attention of regulators. For example, the U.S. Department of Justice recently called for investigations into the healthcare industry’s use of GenAI to analyze patient records for enabling doctors to recommend treatments, drugs and medical devices, and the potential risk of anti-kickback and false claims violations. Lawmakers are also cognizant of complex issues presented by GenAI including, algorithmic data bias and vulnerabilities in data privacy and security. Key governmental stakeholders are evaluating the need to balance technological advancement and ethical responsibility. This being said, GenAI continues to develop at speeds much faster than the legislative pen can scribble. This article evaluates the regulatory trends that address issues of algorithmic data bias and data privacy and security that are inherent to the deployment of GenAI systems in healthcare.

Algorithmic Data Bias

Several companies are exploring the use of GenAI tools to identify patterns and anomalies in electronic medical records, aiming to enhance healthcare efficiencies and diagnostic accuracy. The underlying LLMs in GenAI are trained on extensive datasets, leveraging the analysis of patterns and correlations within the data. However, the precision of these tools and their output accuracy is inherently tied to the quality of the datasets used for their training. Biased or unrepresentative data, and its consequences, has emerged as a primary concern for those seeking to employ these GenAI tools and those who seek to regulate them. Research and studies indicate that training data that is not representative of the broader population (in terms of ethnicity, age, gender, socio-economic status, geographic location, etc.) can lead to biased outcomes, including less accurate diagnoses and unequal healthcare access for underrepresented groups.

Recognizing this inherent issue when using and training GenAI models, the World Health Organization (WHO) through its Regulatory Considerations on Artificial Intelligence for Health (the "WHO Guidance") has stated that "[a]lthough bias, errors and missing data are not unique to AI development, they are nevertheless serious concerns, which may arise for many reasons – including unequal and non-representative training or validation datasets." In the United States, the White House's Blueprint for an AI Bill of Rights (the "Blueprint") labels "Algorithmic Discrimination Protections" as one of the five tenets of responsible AI development and usage. However, it remains to be seen how lawmakers will address these considerations in the form of binding regulation. Additionally, there is a concern that algorithmic discrimination in healthcare could potentially violate civil rights laws, including Title VI and Section 1557 of the Affordable Care Act.

The U.S. Food and Drug Administration (FDA), which currently regulates AI-powered medical devices, has acknowledged the issues related to algorithmic data bias in GenAI models. The FDA's guidance emphasizes the importance of diverse and representative training datasets to minimize biases. Notably, the FDA has not yet granted approval to any device utilizing GenAI. It is yet to be seen how the FDA will apply its considerations for AI and machine learning based medical devices to medical devices powered by GenAI.

Evidently, regulators are recognizing the need for datasets to be diverse and representative in order for GenAI technology to effectively advance the healthcare industry, and that current regulations with respect to AI (i.e., machine learning based AI) lack the nuances needed to achieve the objective.

Data Privacy and Security

In the healthcare context, training data for GenAI models is likely to include sensitive data concerning individual and identifiable patients. The privacy of patients and the security of GenAI systems utilizing patient data are thus paramount concerns. Unsecure GenAI systems not only jeopardize patient safety, but also erode consumer trust in GenAI applications, highlighting the critical need for robust cybersecurity measures to safeguard sensitive healthcare information.

Several governmental and intergovernmental organizations, including the National Institute of Standards and Technology (NIST), WHO and the White House, through its Blueprint, have recognized the need to, and offered guidance on how to protect data utilized in AI systems. NIST published its AI Risk Management Framework which provides voluntary guidance to organizations designing, developing, and deploying AI systems to manage risks, promote trustworthiness, and foster responsible development of AI systems. The WHO has also highlighted the privacy risks associated with GenAI systems and recommends keeping large-scale datasets secure at every development stage. While such guidance is indicative of the industry expectations, it lacks enforceability and merely foreshadows the potential trends and regulations that are necessary to safeguard data privacy and security.

Currently, entities subject to the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (HIPAA) are required to comply with the law when utilizing AI for processing personal health information (PHI), including for training the AI model. A key tenant of HIPAA compliance is having certainty regarding the PHI, who has access to it, and how it's being utilized. As such, HIPAA's Right of Access grants patients the right to access their PHI included in a designated record set. In GenAI systems, however, because of the inherent opacity in the datasets used by the GenAI tool, and the reasoning for the generated healthcare decisions, it is unclear the extent to which a patient may exercise their HIPAA rights.

State-level consumer privacy laws, like Connecticut's Consumer Data Privacy Act (CTDPA) apply when adequate protections are not afforded under HIPAA. For example, the CTDPA affords consumers extensive rights over their personal data, allowing them to 'opt out' of data processing and sales. However, it's crucial to note that CTDPA explicitly excludes PHI from its provisions since protection of this data is covered by HIPAA. Given that the safeguarding of health data under state consumer privacy laws typically applies only in cases where the processor is not classified as a covered entity under HIPAA, the ultimate regulating responsibility may fall back to HIPAA.

Under HIPAA and state privacy laws, transparency in connection with patient data is paramount, however, they may lack clarity as to their application to GenAI, and developers and users of GenAI tools are increasingly seeking guidance as to their obligations and risks. Consistent with current regulations that mandate disclosures of the purposes for which data is used, we anticipate that healthcare providers will likely be encouraged to prioritize transparency in communicating to patients how GenAI algorithms use their data. Although current HIPAA compliant notices may, in most cases, be sufficient to allow for the use and disclosure of PHI in connection with AI-related uses under various treatment, health care operations, or business associate provisions, for abundant caution, where applicable, it may be worth considering if more specific disclosures need to be made with respect to GenAI.

Despite there not being any regulation that is specific to GenAI, recent developments indicate a growing readiness to tackle its legal complexities. As regulators consider how to encourage innovation and efficiencies while ensuring patient safety, maintaining ethical standards, and protecting patient privacy, we anticipate regulatory bodies, such as the FDA, FTC, OCR, and state agencies to direct attention to understanding GenAI technology and developing more future-proof laws. It remains to be seen whether the promising potential of GenAI technology will revolutionize health care or be impaired by regulation.

***

Kritika Bharadwaj is a partner in Day Pitney's Parsippany office and Colton J. Kopcik is an associate in Day Pitney's Stamford office

This article was first published in the New York Law Journal on February 2, 2024.

This communication is provided for educational and informational purposes only and is not intended and should not be construed as legal advice, nor does its distribution or receipt create an attorney-client relationship. This communication may be deemed advertising under applicable state laws. Prior results do not guarantee a similar outcome.

If you have any questions regarding this communication, please contact Day Pitney LLP at 605 Third Avenue, 31st Floor, New York, NY 10158, (212) 297 5800.