DR. CHATBOT: Understanding Regulatory Requirements for Artificial Intelligence in Health Care

By Emma Trivax

Can artificial intelligence (AI) be my new doctor? Maybe. There do not appear to be many guardrails stopping AI from acting as such. Recently, I put various symptoms into an AI chatbot and asked it to diagnose me. The chatbot responded with its best approximation of what was wrong with me, then suggested I follow up with a doctor. I did it a second time, with different symptoms, and it again diagnosed me, then suggested I follow up with a doctor. Is this different from entering my symptoms into Google and seeing the top result from WebMD? Or submitting my symptoms into a symptom checker online? It feels different — likely because the chatbot's response was personally tailored to me. Is this considered practicing medicine?

AI has been making significant strides in the health care sector, offering a range of capabilities from simple language translations to machine-learning diagnoses based on large volumes of patient data. However, the expansion of AI into health care services, devices, and operations presents potential regulatory challenges for health care providers and their counsel.

UNDERSTANDING AI IN HEALTH CARE

AI in health care has a rich history that dates to the 1950s. The earliest applications of AI in this field involved machines that were programmed to make very basic decisions. The 1980s and 1990s saw the development of machine-learning algorithms, which were applied to medical diagnoses, medical imaging, and the prediction of patient outcomes. In the 2000s, the focus shifted to the use of AI in personalized medicine. The 2010s focused on deep learning, which revolutionized AI applications in health care, particularly in the fields of medical imaging, drug discovery, and genetics.[1] Common applications of AI in health care include natural language processing, machine learning, deep learning, generative AI, software as a medical device (SaMD), and clinical decision support software.[2]

REGULATORY LANDSCAPE FOR AI IN HEALTH CARE

No comprehensive federal framework to regulate AI in health care currently exists. Certain states are actively implementing laws to oversee the development and deployment of AI that impacts health care, and approximately half of the states have pending or enacted AI legislation more generally. Michigan, for example, has no AI laws on its books.

On a federal level, the Food and Drug Administration (FDA) regulates the production and sale of medical devices in the U.S., including AI. The FDA classifies medical devices, including AI, into three classes based on risk. Class I is considered the lowest risk category, Class II is considered moderate to high risk, and Class III is the highest risk category.[3] AI software intended to diagnose or treat diseases is considered a medical device, often categorized as SaMD. Depending on the risk level associated with the particular SaMD under review, it can be classified as Class I, II, or III. The FDA also regulates AI software integral to a medical device's hardware. Again, the FDA reviews each new AI software application and subsequently places it in the appropriate class. The FDA review process varies based on the device's risk classification and the nature of any changes made post-market.

The FDA does not review certain types of health-related AI software, including those used for administrative support, promoting a healthy lifestyle, functioning as electronic patient records, and managing data transfer or storage. The 21st Century Cures Act has clarified this by specifically excluding such software from the definition of a medical device, thereby removing it from FDA jurisdiction. This includes clinical decision support software, which provides personalized information to patients and their providers to improve health care outcomes, provided it meets certain criteria. However, distinguishing between software that merely informs medical decisions and software that directly influences medical decisions can be a complex task.

Privacy laws also play a significant role in the use of AI in health care. All applicable federal, state, and international privacy laws need to be adhered to, including the Health Insurance Portability and Accountability Act (HIPAA), genetic information privacy requirements, regulations regarding substance use and mental health services, the General Data Protection Regulation, and state privacy laws.

LEGAL RISKS ASSOCIATED WITH A 'DR. CHATBOT'

As discussed above, the regulation of AI in the health care context is still in its formative stages. This raises significant regulatory and ethical concerns. With few state-specific laws and even fewer federally applicable laws to govern AI's use in health care, several questions are raised. Can AI be used in a way that would be considered practicing medicine? Can AI vendors be held liable for bad medical advice given to patients? Or would the supervising physician, assuming there is one, be held liable? Are there data privacy concerns?

The Corporate Practice of Medicine

The health care industry is heavily regulated, with stringent physician licensing regulations issued by the boards of medicine in each state. Many states also have a "corporate practice of medicine doctrine" (CPOM), which prohibits corporations from engaging in the practice of medicine or employing a physician to provide medical services. This doctrine is rooted in the

principle that a corporation cannot be licensed to practice medicine and therefore cannot exert control over an individual physician's medical judgment. However, individuals licensed to practice medicine may be granted limited corporate structures, such as "professional corporations" (PCs), but such limited corporate structures require the *direct* ownership of the individual(s) licensed to practice medicine.

So, you might ask: How would AI fit into this framework? Health care providers now have access to AI in many different forms. AI can now analyze medical data, provide diagnosis and clinical decision support, and even predict health outcomes. There is certainly potential for the AI vendor or developer to be scrutinized for potentially practicing medicine. Using Michigan as an example, Michigan prohibits individuals from practicing medicine without a license.[4] The practice of medicine means "the diagnosis, treatment, prevention, cure, or relieving of a human disease, ailment, defect, complaint, or other physical or mental condition, by attendance, advice, device, diagnostic test, or other means, or offering, undertaking, attempting to do, or holding oneself out as able to do, any of these acts."[5] If an AI vendor or developer created AI that gave medical advice to treat, diagnose, prevent disease in, or cure a patient, that AI may directly violate Michigan law. While some AI will be used under health care provider oversight, some will not. For instance, in my initial query to the chatbot about medical symptoms, the chatbot did provide a suggested diagnosis without confirmation from a provider first. Despite the AI telling me to follow up with a provider, did the AI just then practice medicine?

Of course, if a provider utilizes the AI as a mere resource before any medical advice is offered to the patient, that may prevent any unlawful practice of medicine by the AI. Providers must remain the ultimate decision-maker, regardless of whether AI is able to come to the same decision. There are many unanswered questions here:

- Who is liable if the physician relies on AI for medical advice that turns out to be incorrect?
- Will AI vendors put disclaimer language in their agreements prohibiting users from practicing medicine with the AI?
- Is that disclaimer enough?

These are the types of questions that will only be answered as the practice of using AI in health care increases. The disparity between the stringent regulation of the CPOM and the relatively lax oversight of AI in health care is stark.

Privacy Laws

Michigan has enacted the Identity Theft Protection Act, MCL 445.61-79d. This law requires businesses and government agencies to take certain measures to protect personal identifying information. For example, it is a prohibited act to use another person's personal identifying information to obtain credit, goods, services, money, or medical records with intent to defraud or violate the law.[6] Violations of this act can result in civil penalties. Health care providers must remain vigilant that they understand how the AI companies are using their patients' information. A use of patient information that may be permitted in one state could be a violation of Michigan's law.

There also are concerns about how HIPAA applies to AI. HIPAA was enacted in a time when paper records were the norm, and it did not fully address the digital transformation of health care. Nonetheless, practitioners have found ways to adapt their physical, technical, and administrative safeguards to keep up with the ever-changing technological environment. However, AI is less self-contained than many electronic medical record systems and may make it more difficult to adequately protect against bad actors. Just in the last four years, there has been a 239% increase in large breaches that resulted from hacking activities, and there has been a 278% increase in ransomware across the board. In 2023, 77% of the large breaches reported to the Office for Civil Rights resulted from hacking.[7] As such, AI companies must embrace appropriate security measures, monitor compliance, create stringent access controls, and provide comprehensive training for their personnel and associated vendors. Health care practitioners must always be cautious when introducing a new technology into their practices.

Cultivating trust in these technologies is pivotal for their enduring utility and success in health care, and this trust is intricately linked to safeguarding the privacy of patient data. The input of protected health information into AI software could be considered an unauthorized disclosure under HIPAA, if the AI company has not signed a business associate agreement (BAA) with the health care provider. Furthermore, AI companies must adhere to the terms of the BAA when using or disclosing protected health information. For instance, if an AI company uses protected health information to enhance its algorithms in a manner not permitted by the BAA, it would constitute a HIPAA violation.

AI Biases

The World Health Organization cautioned AI users in the health care field that "the data used to train AI may be biased, generating misleading or inaccurate information that could pose risks to health, equity and inclusiveness."[8] The California attorney general also has launched an inquiry into potential racial and ethnic disparities in commercial health care algorithms used by hospitals and health care providers. This all underscores the urgent need for comprehensive regulatory guidelines to ensure AI is used responsibly and ethically in health care.

CONCLUSION

The use of AI in health care is a rapidly evolving field housed in a complex regulatory landscape. Even without definitive answers, health care providers and their counsel must attempt to understand the relevant regulatory requirements to ensure compliance and mitigate risks. As AI continues to advance and become more integrated into health care services, devices, and operations, it is essential to stay informed about the latest regulatory developments and guidelines.

Emma Trivax is an attorney in Troutman Pepper's Detroit office. Emma represents a wide range of health care providers, including physicians, pharmacies, hospitals, clinical laboratories, skilled nursing facilities, DMEPOS suppliers, and more. She advises her clients on regulatory, transactional, and compliance matters, including mergers and acquisitions, fraud and abuse, HIPAA, corporate practice of medicine, billing/reimbursement, and licensing issues.

Footnotes:

1. Vivek Kaul, Sarah Enslin, and Seth A. Gross, *History of Artificial Intelligence in Medicine*, GIE Journal (2020).
2. *Artificial Intelligence for Health Care Providers: Overview*, Practical Law Health Care, Westlaw (last accessed Nov. 1, 2023).
3. *Regulatory Controls*, U.S. Food & Drug Administration, <fda.gov/medical-devices/overview-device-regulation/regulatory-controls> (last accessed Nov. 1, 2023).
4. MCL 333.17011.
5. MCL 333.17001(1)(j).
6. MCL 445.65(1)(a)(i).
7. *HHS' Office for Civil Rights Settles Ransomware Cyber-Attack Investigation*, U.S. Department of Health and Human Services, <https://www.hhs.gov/about/news/2023/10/31/hhs-office-civil-rights-settles-ransomware-cyber-attack-investigation.html#:~:text=Ransomware%20and%20hacking%20are%20the,large%20breaches%20reported%20to%20OCR.> (last accessed Nov. 2, 2023).
8. *WHO Calls for Safe and Ethical AI for Health*, World Health Organization, <https://www.who.int/news/item/16-05-2023-who-calls-for-safe-and-ethical-ai-for-health> (last accessed Nov. 7, 2023).