

Rise of medical AI poses new legal risks for doctors

■ Cite as: *CMAJ* 2019 October 21;191:E1173-4. doi: 10.1503/cmaj.1095823

Posted on cmajnews.com on Oct. 2, 2019

The use of artificial intelligence (AI) in medicine is expanding beyond regulatory and legal checks, and doctors may find themselves on the hook when things go wrong, warned experts at the Canadian Medical Protective Association's (CMPA) annual meeting.

"It's not the technology that's going to put you at risk; it's the policy around it," said Dr. Hartley Stern, CMPA's executive director and CEO. "We have to get legal and regulatory clarity."

It may take years to get regulatory and legal safeguards in place, but that isn't slowing the uptake of medical AI. Earlier this year, the Mayo Clinic announced a partnership with Google to use the hospital's patient data in the company's AI experiments, despite similar partnerships running into trouble over privacy breaches.

Whether or not doctors are ready to use AI in their practices, "it is just going to be impossible to ignore," Stern said.

In so far as AI improves care, it will reduce some medical-legal risks. For example, "we spend on average per year about \$150-\$160 million on lawsuits in hypoxic brain injuries for babies," Stern explained. "It would be unbelievably helpful if we can determine what are the in-utero events that are leading to this versus what are the intra-partum events."

Artificial intelligence may also help reduce physician burnout, and thereby the potential for medical errors and complaints, by easing administra-

tive burdens through smarter electronic health records and digital scribes, he said.

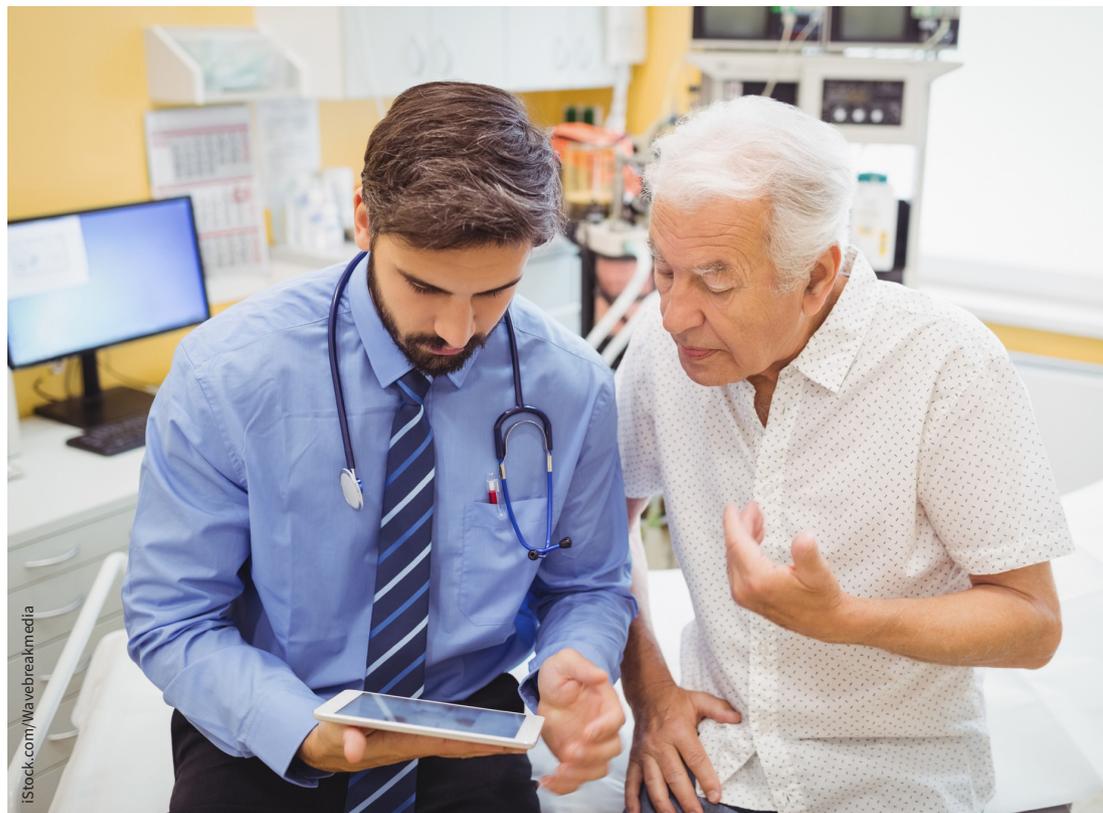
However, evidence about the effectiveness and reliability of medical AI remains limited, and no one is regulating the technology. Under current laws, it's up to doctors to assess the usefulness of information derived from AI, and doctors are liable if errors occur, Stern said. Ultimately, the buck stops with the physician, "not the machine."

According to Dr. David Naylor, professor of medicine and president emeritus at the University of Toronto, this poses a problem because doctors may lack the

technological savvy to assess the safety and effectiveness of AI. "You're not a statistician; you're not a computer scientist; you're not a deep learning expert."

Even for experts, it's often impossible to unpack an algorithm's underlying reasoning because it's too complex or it's protected as a trade secret. "There's a black box problem here," Naylor explained. "You can't unbundle them in the easy way a statistic can be pulled apart and the variables isolated."

Stern noted the matter is further complicated because algorithms that prove reliable when trained on data from one population may not be applicable to



Doctors are still liable for errors in care caused by artificial intelligence, the Canadian Medical Protective Association cautions.

other populations. For example, medical AI that outperformed clinicians in diagnosing skin cancer was trained mostly on data from white patients. “When the same kind of diagnostic algorithms were applied to people of colour, the accuracy dropped dramatically.”

Doctors unaware of such biases may be misled by medical AI. In one recent case, leaked internal documents showed that IBM’s Watson supercomputer made “unsafe and incorrect” cancer treatment recommendations. The company traced the problem to engineers training the AI on hypothetical patient cases instead of real patient data.

According to Naylor, intellectual property protections and privacy laws pose a barrier to external validation of the data

companies feed their algorithms. “It’s going to require a bit of concerted effort to work with privacy commissioners and patient representatives to come up with rules for this game.”

Yet those same privacy laws impose few checks on how AI vendors use patient data, especially if that data is stripped of identifying details. A recent legal challenge to a data-sharing partnership between Google and the University of Chicago Medical Center highlighted how the company could theoretically combine deidentified records with its vast stores of geolocation data, search queries and social media posts to reidentify individuals.

According to Naylor, one way to balance these access and privacy challenges may be to establish data trusts that would

manage health information on behalf of patients and physicians based on shared terms and conditions.

Stern noted that physicians will also need training in how to assess and apply AI, and how to communicate with patients about the role of AI in diagnoses and treatments. “The biggest cause that we see in college complaints is the inability to communicate what you’re trying to do for the patient,” he said. “Communication of how this algorithm is fitting into your practice, that communication is going to be pivotal.”

Lauren Vogel, CMAJ

Editor’s note: Dr. David Naylor is a member of CMAH 2018 board, which oversees all CMA subsidiaries. He was not involved in the decision-making for this article.