KEY AUTHORS

Risa M. Kirshblum
PRACTICE GROUP LEADER
416-865-3098
rkirshblum@litigate.com

Jaan Lilles
PRACTICE GROUP LEADER
416-865-3552
jlilles@litigate.com

Colin Johnston
PARTNER
416-865-2971
cjohnston@litigate.com

Christina A. Papageorgakopoulos
ASSOCIATE
416-865-3700
cpapageorgakopoulos@litigate.com

OUR PROFESSIONAL LIABILITY & REGULATION EXPERTISE

Lenczner Slaght has one of the leading professional liability practices in Canada, representing clients in diverse fields across a broad landscape of regulatory, civil and quasi-criminal matters. We defend professionals before disciplinary and regulatory tribunals and in all levels of the courts across the country. We also prosecute professional disciplinary cases for many regulatory colleges and governing bodies. In addition, we act as general counsel to several of those bodies.

Professional Liability

"Professionals who use AI in their practices should understand they must use this technology competently or risk regulatory scrutiny."

What were professionals thinking about in 2025, and why?

In 2025, professionals were thinking about the privacy risks presented by new information technologies; namely, the unique and emerging risks associated with AI tools.

A recent analysis by Statistics Canada found significant growth in expected AI usage in the business, finance, insurance, and healthcare sectors. These tools present clear benefits. For example, an Ontario MD study found that "AI scribes" reduced physicians' time spent on paperwork by 70 per cent.

However, the benefits of these technologies are accompanied by novel risks that can be difficult to anticipate.

A recent privacy breach considered by Ontario's Information and Privacy Commissioner (IPC), Reported Breach HR24-00691, provides an excellent example of this. In this case, a hospital-based physician who relinquished his privileges and left the hospital had inadvertently retained a calendar invitation to a departmental rounds meeting on his personal digital calendar. The invitation contained a videoconference link associated with his personal email address. Months after leaving the hospital, this physician downloaded a publicly available AI-based transcription tool to his personal phone. On the date of the meeting, and unbeknownst to either the physician or the hospital, this AI tool accessed the videoconference link in the physician's personal calendar, "attended" the hospital's specialty rounds using the physician's personal email address, and recorded the meeting. The tool then autonomously circulated a transcription of the meeting to all attendees, including the physician who no longer held privileges at the hospital. This privacy breach underscores the significant risks associated with "AI autonomy."

What's the primary takeaway for professional service providers?

Professionals who use AI in their practices should understand they must use this technology competently or risk regulatory scrutiny. For example, the Law Society of Ontario's practice note recognizes that generative AI is a valuable tool but requires that professionals take the time to understand each tool's capabilities, limitations, and terms of use. The IPC case discussed above is an excellent example of the privacy risks that can be associated with the use of poorly understood and inadequately managed AI tools. While the IPC imposed no fine or sanction, it issued extensive and pointed recommendations to the hospital that are well worth heeding. Among other things, professional service providers should ensure they have robust policies establishing:

- Clear and enforced expectations for vetting and using AI-based tools in individual practice or by staff.
- Controls over the use of personal digital devices, accounts, and online services in connection with any workplace information along with safeguards to ensure client information is confined to secured workplace digital infrastructure.
- Offboarding processes that immediately revoke all access to sensitive information, including access to calendar invites, upon departure by a professional or staff member.

What's one trend you are expecting in 2026?

Expect regulators and the courts to respond to the risks presented by increasingly autonomous AI tools by prioritizing the protection of clients' interests and imposing corresponding obligations on professionals and professional services firms. While the increasing prevalence and sophistication of cyberattacks by bad "human" actors is well understood, significant legal risks can arise from the uncritical use of AI tools that can act without a "human in the loop." Professional service providers would be well advised to get ahead of the curve by adopting procedures to oversee and manage the integration of these tools into their information systems. Those who fail to do so risk becoming unwilling parties to interesting future legal developments before the IPC or the courts.

Lenczner Slaght