Are employers doing their due diligence in offering virtual care?

'If we recognize the benefits of this, we equally have to recognize the potential harms and risks,' says academic involved with Canadian study

By Sarah Dobson
Feb 22, 2024

They exploded during the pandemic and have established themselves as a staple in Canada's health care.

Virtual care platforms — or telehealth or telemedicine — provide a convenient, accessible option when many people lack a family physician or the time to visit one.

As a result, many employers offer the service as an employee benefit.

But are they doing their due diligence? Because a recent Canadian study suggests virtual care companies use the data collected from patients to market other products and services. In some cases, they say the vendors are funded by pharmaceutical companies to analyse the data collected from patients and adjust care pathways, with the goal of increasing uptake of a drug or vaccine.

The study was based on interviews conducted between October 2021 and January 2022 along with publicly available documents on websites of commercial virtual care platforms.

And while participants described these business practices as expected and appropriate, some were concerned about patient privacy, industry influence over care and risks to marginalised communities.

"In Canada and elsewhere around the world, it's widely recognized that health information is particularly private, sensitive information," says Brenda McPhail, co-author of the study and director, executive education, public policy in the Digital Society Program at McMaster University.

"So we were hoping that those platforms providing health information would be taking those social expectations and legal obligations into account. And what we found was there were still a lot of ways in which patient information was being used in a for-profit model."

De-identifying data in virtual care

The research found there are three types of data collected by companies with virtual care platforms: personal health information, registration-related data (such as name, address, gender, birthdate) and de-identified personal information.

But a lot of companies use the personal health information to create de-identified data, and use that for analytics or other purposes, says Sheryl Spithoff, co-author of the study and assistant professor, Department of Family and Community Medicine, University of Toronto.

“And that data, there's very few legislative protections for. So some companies would just state straight out, essentially, once it's de-identified, ‘It's ours, and we can do whatever we want with it.’ And that's, of course, concerning. Even though there's guidance around what data are de-identified, the risk is supposed to be low, there's no clear standards, and what does ‘low’ mean?”

With de-identification of individuals, there’s always the risk of data being hacked and ending up in the wrong hands, she says.

“And even if the data remain de-identified, it can still be used… to make inferences about groups. And if the social context isn’t considered, the data could incorporate social biases and perpetuate bias and harm.”

Health privacy legislation and virtual care

When it comes to health privacy legislation in Canada, there are different pieces of legislation for the different provinces and territories, plus there is the “added complication” of federal regulation — the Personal Information Protection and Electronic Documents Act or PIPEDA — for commercial vendors of technology, in order to collect and use data in the course of their commercial activities, says McPhail.

And the “fuzzy” part involves the registration information, which people provide to connect to the platforms and to find health care providers.

“We're accustomed to thinking of the information that we share with our healthcare providers as being protected by legislation. And the average patient wouldn't think about that if they connected online, that that could be any different,” she says.

“But, legally, it actually is a little bit different because of gaps in the laws that just didn't foresee using these kind of platforms in this way.”

Many companies do not consider registration information as health information, but the research suggests this needs a higher level of protection, says McPhail.

“This is an area where privacy law doesn't do a good job of protecting us, because privacy law focuses on personally identifiable information. But the reality is that data and artificial intelligence and analytics allow really granular inferences to be drawn about whether or not we are a member of a particular group, whether we are like others and a particular category that allows for targeting of us and our behaviour in ways that ultimately is very personal.”

Sharing health information for marketing purposes

The type of things that are being recommended through these platforms are private pay services, which have more of a markup, says Spithoff, “and companies are able to make more money often, which is why those are the services that they're promoting.”

Some companies also share this information with third parties for marketing and advertising purposes, she says.

“Almost all, from reviewing privacy policies, share information like IP addresses, device identifiers, browsing history, that type of personal information with companies like Facebook and Google, who then of course use it for marketing and advertising. Some companies also shared information like names and email addresses with third parties for marketing and advertising purposes.”

Some of the participants in the study also said their platforms partner with pharmaceutical companies, and they were using patient data to promote the pharmaceutical company's product, such as a drug or vaccine, through the platform, says Spithoff.

“They did things like sending out reminders, adjusting the frequency of the reminders of visits of the platform interface — all with a goal of promoting that drug or vaccine. And then they would evaluate the data to see ‘Was this effective? Did it get more patients to take this drug or vaccine?’ And then [they were] tweaking that until it was optimized.”

Concerns about quality of care in telehealth

This is where the researchers had concerns around the quality of care, when a pharmaceutical company in some way is funding the platform, and adjusting how they're providing care with a goal of increasing that product uptake by patients, she says.

“[Participants] said that they feel that one of the reasons, perhaps, that patients are agreeing or not looking into these privacy policies more closely is because these are largely physicians who are licensed in the provinces in Canada, and they have trust that their data are being handled the same way as if they walked into a hospital or something like that.

“And that trust, of course, it's essential to providing a health care service, and we're concerned that it's not being treated appropriately.”

Physicians have a fiduciary responsibility to patients to put their care first, and they also are subject to regulation from their colleges, whereas private companies don't have those same kinds of responsibilities, says Spithoff. “Their responsibilities are to shareholders.”

The virtual care platform or telehealth provider itself is part of the care journey, says McPhail.

“We found that the platform would do things like send reminders to adjust timing of visits, to encourage tests or potential tests in labs. There was a greater, I would say, potential for intervention in the health journey than if you're just talking with your single doctor and your doctor is talking to a pharmaceutical representative, instead of a quantitative difference based on

the data collection potential, and then the leveraging of the platform as a way to influence people's behaviour in terms of the way that they seek care, and they asked for care, and they take up recommendations."

Opting out and transparency in healthcare

So how much do employees know when they're accessing these virtual care services?

The researchers found that often the platform's relationships with third parties is not made clear, which is "very problematic," says Spithoff.

"This is an area where we definitely need transparency at a minimum. And what we're recommending is that it should be banned," she says.

"Physicians aren't allowed to take money in exchange for prescribing drugs. To me, it doesn't make sense that a company would be allowed to take money in exchange for trying to increase the uptake of a drug or vaccine."

Most of the privacy policies are long and dense, and while they may provide instructions on how to "opt out" out of emails, "it was unclear if you could opt out of having the data used in the first place," says Spithoff.

People go to see their doctor when they need care of some kind, which means they are often in a vulnerable state, says McPhail.

"And that's not the kind of state that is amenable to thinking, 'Oh, what's going to happen If I click here?'" she says.

"They're catching people at a time when they're particularly vulnerable and likely to not be worried about the privacy of their health information, particularly in Canada because we're really used to believing that that information is very well protected by our laws because it has been a public service."

Recommendations for HR in improving virtual care

When it comes to fixing or challenging some of these concerns about virtual care platforms, at a minimum, there needs to be greater transparency and understanding about what's going on here, says Spithoff.

"One thing we're recommending is that all data collected through the platform be treated as personal health information, that we give additional protections to the data," she says, along with having mechanisms to ensure that pharmaceutical companies can't fund the platforms in order to promote the uptake of their products.

In addition, for HR, due diligence in this area is essential, says Spithoff.

“They should be carefully reading through those privacy policies, ensuring that patients don't have to agree to these non-essential uses of their data, making sure that the platform is not sharing any information with third parties, that patients aren't continually being subjected to marketing of other products and services, upselling things that... aren't covered and might not provide them any benefit, but maybe feel an obligation or to purchase or engage with.”

Also, HR should better understand what the platforms are doing with de-identified data by asking key questions, she says.

“Who's using it? How is it being stored?” she says. “And then [it’s about] asking a platform ‘Do you have any relationships with pharmaceutical companies? Is there any partnership, involvement, sponsorship happening there? And if there is, what's the nature of that relationship?”

The HR community is on the front lines of protecting people because it’s in the position of being part of the negotiations, says McPhail.

“Companies should be legally obliged to share with you the ways that they're collecting and using information. And if you don't ask, you're not going to find out. If you do ask, you have the opportunity to negotiate contractual terms that are to the benefit of your client base.”

In the end, the point of this research is not to say that these platforms and services aren’t fulfilling a need in our healthcare systems, she says.

“[It’s] merely to say they've taken off really quickly… let's think this through. If we recognize the benefits of this, we equally have to recognize the potential harms and risks.”