+BUSINESS | In print

Practices must prioritise privacy to do AI well – especially for Māori

Michael Webster

💬 0

Friday 5 April 2024, 01:54 PM

3 minutes to Read

AI tools are helpful, but patient records must be protected, especially regarding information-sharing with a third party [Image: MicroStockHubon iStock]

Privacy is paramount when integrating AI into healthcare, particularly concerning Māori patients. **Michael Webster** explores how to leverage AI tools while preserving patient confidentiality and trust

AI can, and likely will, become another tool in the primary healthcare toolbox

The fundamental relationship between a patient and their GP is one of trust. Trust that you are medically skilled, that you’re going to investigate my ailment with integrity, and that you keep what happens in your clinic confidential.

However, I also know that GPs have increasing numbers of patients, often with complexities, that you can spend your lunch breaks and weekends doing paperwork, and that sometimes you’re also running a business.

So, you could do with a helping hand, which for some might come in the form of using artificial intelligence tools. I see some American clinics are now doing that (mainly for paperwork), and they report they are more efficient, which means being able to see more patients a day.

I wrote in my 11 October column about the essentials of AI and privacy, and I’d like to build on that here.

Let’s look at a tool involving writing up clinic notes. You’ve asked the patient’s permission before using AI during your consult, and they’re happy with that. However, from a technical point of view, including someone’s personal information in prompts for an AI tool could mean that this information is collected and re-used for other unintended purposes, such as training new AI tools.

At the very least, you should research the provider’s contractual terms and privacy policy and ensure that your patient’s information is protected at each stage.

But before you even begin, I recommend doing a privacy impact assessment for the clinic to determine what you’re collecting, why, and how you’ll mitigate any risks. It’s also essential in this work to consider Māori perspectives on privacy. And be proactive about how you engage because I have heard specific concerns about Māori privacy and AI tools, including:

collection of Māori information without work to build relationships of trust

exclusion from processes and decisions around adopting AI tools that affect Māori whānau, hapū and iwi

concerns about bias from systems developed overseas that do not work accurately for Māori.

Adopting AI tools that are not designed for and in consultation with our communities may lead to inaccuracy in the form of bias, exclusion (particularly of poorly represented groups) and other privacy harms.

At the core of the Privacy Act 2020 are the 13 information privacy principles (IPPs) that set out how agencies must handle personal information. The IPPs govern the activities of collecting, using and sharing personal information. They apply whether you're building your own AI tools, using AI tools to support decision-making or have team members who are informally using AI in their work. Of course, in the health sector, the IPPs are modified and replaced with the 13 Health Information Privacy Rules in the Health Information Code 2020, with more restrictive requirements reflecting the sensitive nature of health information and the trust required for the therapeutic relationship.

Using AI tools within organisations may unintentionally lead to more information sharing with third-party providers, as team members supply images, text prompts and other data. Some AI tools can leak sensitive information, which increases security risks.

You must know all this and do your due diligence before making informed decisions.

Also, any “permission” provided by your patient is fully informed and can be relied upon.

AI tools can also make it easier for criminals to impersonate real people, create fake identities online and automate hacking and phishing campaigns, which all still rely on tricking real people. Are your existing security measures up to scratch? What additional safeguards would you need to implement? How savvy are your staff about these scams?

The nature of your work means accuracy is critical. You will have read about situations when AI tools generated fake or unreliable information. To uphold the trust that patients place in you, you must think about how a responsible person checks that the outputs from tools are accurate and uphold patient welfare, and then empower and adequately resource them to do the job.

Overall, it may help to think about using AI in ways that uphold accountability for people in your organisation, your customers and the broader community.

Questions about where and how patient information is used might be good to raise with your colleagues and across your practice to make sure that all the digital tools you use meet your and your patients' expectations.

Where people have responsible roles, which most people in primary healthcare will, any use of AI tools should maintain and complement those responsibilities.

AI can, and likely will, become another tool in the primary healthcare toolbox. But take the time to build a patient-centric model now with privacy at the heart of its design. Forewarned is forearmed with AI and healthcare.

Michael Webster is the privacy commissioner