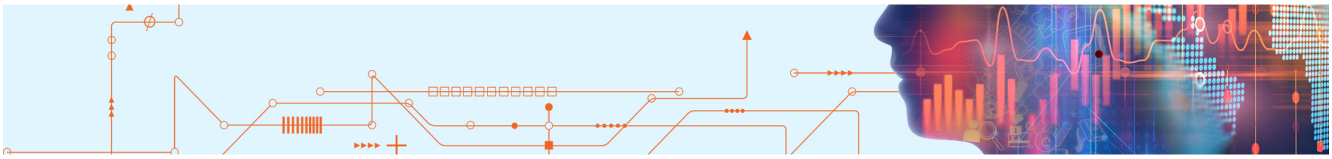

Handling Patient Data in Artificial Intelligence

March 10, 2020

By Amanda Branch and Noel Courage

There has been a vast expansion in the use of AI in healthcare. There are many privacy issues that accompany unlocking the potential of AI. An AI system requires lots of data in order to work properly by changing its behavior on information or experience. Since patient data may contain personal information, there are real concerns about the privacy implications of AI, such as the requirements for personal information to be used, and what privacy and security measures are required to protect that data.

Many AI technologies are developed and tested in a multi-disciplinary manner. Hospitals collaborate with companies. Computer experts cooperate with clinicians. The backers of the technology are often focused on the deal, the technology and IP issues. It is important for lawyers to make clients aware of the health privacy implications at the outset of collaborations and transactions, not once they are well underway. Key issues can involve patient consent, handling of data and retention of data. The consequences of mishandling privacy issues or a privacy breach can be significant, and difficult to remedy.

The Toronto Computer Lawyer's Group ("**TCLG**") is having a lunch seminar on this issue March 11, 2020, called "**Personal Health Information: Artificial Intelligence and its Use of Health Data**" (click here for details). The speakers are Rosario Cartagena of ICES (formerly the *Institute for Clinical Evaluative Sciences*) and Michael Watts of Osler.

Under the federal *Personal Information Protection and Electronic Documents Act*, ("**PIPEDA**"), the collection of personal information must be limited to that which is needed for the purposes identified by the organization. AI developers may prefer to maximize the data pool and retain data for long periods of time. Personal information should be retained only so long as necessary to fulfill the reasonably stated purpose for which it was initially collected. Indefinite retention is generally not considered appropriate.

There are also challenges around how to obtain valid (meaningful) patient consent to providing data for use in a complex technology that creates an output without human intervention. The Office of the Privacy Commissioner of Canada published general guidance for obtaining meaningful consent. Read more on the Guidelines here. A goal is to achieve transparency in the context of AI. Developers and their users (e.g. hospitals) should incorporate and consider privacy principles at each step in the design and implementation process (known as Privacy by Design). Notification to consumers should be done in a user-friendly way, such as using clear language, layered policies and just-in-time notices at the point where particularly sensitive data is being collected.

The law is often slow to adapt to new technologies. Lawyers need to be prepared to consider privacy at each step of AI development, to keep developers, users and their products on track.

Content shared on Bereskin & Parr's website is for information purposes only. It should not be taken as legal or professional advice. To obtain such advice, please contact a Bereskin & Parr LLP professional. We will be pleased to help you.