

## Artificial Intelligence: Innovation Procurement and Legal Questions

Denis Chamberland, Principal, Chamberland Law Corporation<sup>1</sup>

Some months ago, Mackenzie Health launched an innovation procurement to acquire artificial intelligence (AI). AI is simply software, but software that harnesses big data analytics, which is the process of examining large and varied data sets (*i.e.*, a collection of related sets of information) to uncover hidden patterns, unknown correlations, market trends, individual preferences, and other useful information that can help organizations make better informed business and clinical decisions. The exponential growth in machine processing power in the last few years has enabled the technique of machine learning, in which computers learn by example and teach themselves to carry out pattern recognition tasks without being explicitly programmed to do so. Healthcare is now regarded as a highly promising sector for AI.

Mackenzie Health's innovation procurement was initiated to address the province's privacy and security requirements. As the province embraces universal Electronic Health Records for all Ontarians, a significant challenge for hospitals relates to the handling of the ballooning volume of personal health information. The growing mass of information that privacy officers need to deal with is daunting, particularly in light of the guidance issued by the Information and Privacy Commissioner of Ontario (IPC) directing hospitals to audit all accesses to personal health information in electronic systems. The IPC's guidance was issued in the aftermath of the launch of a \$412 million class action lawsuit in 2014 after a hospital admitted to privacy breaches resulting from two employees selling patient information over a two-year period.

To ensure it has the capacity to comply with the IPC's guidance, Mackenzie Health sought to procure a health record privacy solution that not only meets the IPC's auditing requirements, but also proactively identifies trends and strategies to prevent future unauthorized access, promotes real-time access to shared patient records, and improves the cost-efficiency of care delivery. By contrast, conventional technology solutions focus on simple rules-based auditing, which can result in a very large number of false-positives needing to be manually reviewed, an impossible task to achieve in real-time.

With the objective of leveraging big data analytics and machine learning, Mackenzie Health tapped the market to procure a solution capable of conducting audits in real-time, of performing autonomous and/or semi-autonomous event analysis to maintain a low false positive rate (with a high accuracy rate), and of providing a range of tools to expedite the investigative

---

<sup>1</sup> Denis Chamberland is a commercial lawyer with extensive procurement, technology and trade law experience in the healthcare sector in Canada and Europe. He worked with Mackenzie Health in the above-described AI innovation procurement and has advised on the Competitive Dialogue in Canada and Europe. He is presently with Fogler, Rubinoff LLP

process. This, it is hoped, will slow or reduce the growing cost of privacy compliance and transform privacy auditing from a reactive after-the-fact investigation model to a pre-emptive, real-time protection model.

To procure its health record privacy solution, Mackenzie Health's project team adeptly leveraged the Competitive Dialogue, a highly effective type of innovation procurement flagged by the Ontario Centres of Excellence. Although new to Canada from Europe, the Dialogue's procedure allows a buyer to hold separate but contemporaneous negotiations with qualified parties. Unlike the classic request for proposals (RFP) process, where only the solution described in the RFP is considered, the Dialogue produces a variety of different and more responsive solutions, though it requires a good knowledge of the legal procedural fairness duties.

Here the buying hospital and each bidder collaborate in real time to devise a solution that truly meets the needs of the hospital. "We had a common problem that required an innovative solution and the Dialogue provided the flexibility we needed to achieve our goal", said Richard Tam, Executive Vice President and Chief Administrative Officer of Mackenzie Health.

The legal aspects of procuring AI raise substantial challenges for law and policy makers, as the law struggles to catch up. Procuring AI is more complicated than procuring a physical product or off-the-shelf software. What is being procured specifically should come from an interchange with the market, which an RFP does not easily accommodate.

The Competitive Dialogue process is well suited for defining complex needs in the healthcare sector and is one that hospitals should embrace. But attention will need to focus on how the Dialogue works with the procurement requirements set out in the newly-promulgated trade agreements that apply to hospitals across Canada (see the Canadian Free Trade Agreement, which came into force on July 1, 2017, and the Canada-European Union Comprehensive Economic and Trade Agreement, on September 21, 2017). In Ontario, the rules set out in the Broader Public Sector Procurement Directive apply to provincial procurements.

Any contract for the purchase of AI almost inevitably requires a 'bedding-in' period to allow for deep learning, the process in which large datasets are fed into the AI software to accurately recognize patterns from the input data. Once trained, the software's decreasing error rates gradually allow it to make more accurate predictions. If the AI software fails to reach the targeted level of predictive analysis during the bedding-in period, a contractual exit ramp should be available to the hospital. The legal consequences of such an exit need to be accounted for.

There is also data law, which is at the heart of AI. Data privacy and security are now prominent in the business world, but of equal importance are the legal rights and duties around data licensing (which party to the contract has the necessary permissions to do what they are aiming to do with the data?) and data ownership (which party owns the data that is produced from the AI software?). And with AI software, there is the question of whether the software is regulated as a medical device under the federal *Food and Drugs Act*.

For now, AI is so new that the focus is still on getting the basic details of the deep learning phase right, such as agreeing on realistic expectations in the statement of work. But the tide is now turning to addressing the legal issues, particularly as these relate to the allocation of the liabilities. For instance, what is the balance of rights and responsibilities between the hospital and its AI software provider, its cloud service provider, and any third-party research institution, if one is involved? And should liability be governed entirely by contract or will negligence law also play a role?