A guidance for novel ethics of privacy issues associated with artificial intelligence in the public sector research domain[1]

Authors (in alphabetical order): Ciaran Aiken, Sarah Flann, Holly Longstaff, Stephania Manusha, Sasha Pavlovich, Janet Scott, and Joleen Wright

Background

Artificial Intelligence (AI) can be described as machine performed tasks using big data[2] to produce data-driven decision support for clinical care, research, and corporate organizational services such as auditing. Some AI uses algorithms to identify patterns in data and that is the primary focus of this guidance. The information provided here aims to be technologically agnostic. The issues raised are intended to help direct attention to novel ethics of privacy issues associated with AI in the research domain, but they may have broader applications. This guidance provides a basis for discussion for those working in the public sector research domain in British Columbia (BC) but does not replace the need for in-depth analyses and institution-wide strategies, which are desperately needed in this area.

It is vital that multi-scale governance mechanisms are developed for AI in research that permits administrative and scientific leadership to understand the full impact of AI within their program or institution so that they can make strategic, fully informed decisions. Leadership should be encouraged to use their corporate resources including legal, ethics, privacy, security, regulatory, and risk offices as well as their Research Ethics Boards, clinical research agreements offices, and data management experts. They may also wish to draw on local, federal, and international resources such as the June 2021 joint special report *Getting Ahead of the Curve: Meeting Challenges to Privacy and Fairness Arising from the Use of Artificial Intelligence in the Public Sector* prepared by the Ombudsperson of BC, the Information and Privacy Commissioner of BC, and the Ombudsman and Information and Privacy Commissioner of the Yukon Territory.[3] Other key resources include the *Declaration on Ethics and Data Protection in AI* established at the 2018 International Conference of Data Protection and Privacy Commissioners[4], the 2019 *Ethics Guidelines for Trustworthy AI* presented by the European Commission's High-Level Expert Group on AI (AI HLEG)[5], the UK Government's *Data Ethics Framework Template*[6], and the work of CIFAR,[7] who has been appointed by the Government of Canada to develop a *Pan-Canadian AI Strategy*, the world's first national AI strategy.

Emergent themes

The following is a list of themes that emerged from a literature review conducted in this area. These interconnected themes highlight key considerations and questions that ought to drive discussions around any type of AI to help avoid unintended and unethical consequences.

---

[1] This guidance will be regularly reviewed to ensure relevance to the changing AI landscape.

[2] While consensus has not been reached, big data is often characterized as including the four V's; volume, veracity, variety, and velocity (see-Galetsi, P., Katsaliaki, K., & Kumar, S. (2020). Big data analytics in the health sector: Theoretical framework, techniques, and prospects. International Journal of Information Management, 50, 206-216). Fundamentally, big data's size exceeds the capacity of traditional methods of data storage, analysis, and management (see-Trnka, A. (2014). Big Data Analysis. European Journal of Science and Theology, 10 (1), 143-148.).

[3] Please see: 3546 (oipc.bc.ca)

[4] Please see: 40th International Conference of Data Protection and Privacy Commissioners, Brussels (globalprivacyassembly.org)

[5] Please see: Ethics guidelines for trustworthy AI | Shaping Europe's digital future (europa.eu)

[6] Please see: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/917779/Data_Ethics_Framework_editable_template.odt

[7] CIFAR works with universities, hospitals, and Canada's three national AI Institutes: Amii (Edmonton), Mila (Montreal), and the Vector Institute (Toronto). For more information please see: Pan-Canadian AI Strategy - CIFAR

Theme	Recommendation
Data quality and assessment	
• Quality and assessment (statistical testing and validation) – What is not scientifically valid cannot be ethical. Correct scientific expertise is needed to ensure that models are robust and validated accurately. • Training of the algorithm –It is vital to use complete datasets that will not result in unethical outcomes (those that are racist or sexist for example). What are the appropriate benchmarks and standards? Are the data generalizable beyond our site? • Quality is always interconnected and underpins everything and all other themes. Checks and balances are essential. Researchers using AI need access to good quality data. • How can you correct or withdraw data when systems are so integrated?	• Consult with data experts and clinicians early on and throughout the lifecycle of the AI initiative. • Develop training materials and methods for those engaged in AI.
Perceptions and norms	
• Are we being transparent with our use of AI? Are we violating any public norms? Who should be contributing to and influencing these decisions? • Socio-technical influence –AI may have an influence on medical practice and how we understand evidence and make decisions. There is a need for checks and balances on how AI translates into future research and clinical processes. AI may become a catalyst for change with methods, protocols, processes, etc. • The role of human control (delegating to the machine) may cause concern for patients and publics. • There is a need to address compliance norms and the historical discomfort many have with hypothesis driven research. • When is it permissible to use fully identifiable information with AI? • Under what conditions should we be partnering with industry?	• Engage with patient partners and patient experience experts across your organization. • Engage with your local Research Ethics Board and ethics experts to inform them about AI and co-develop new methods and approaches for reviewing AI. • Engage with physicians to ensure that the AI being contemplated will not only be valuable for them in their practice but will also be accepted by patients.
Access	
• Ability to access the right data at the right time is essential for AI in research. • We must consider just distribution of limited resources and ensure equitable access to AI itself that is fair for all types of research.	• Create good data repositories. • Create transparent and equitable publicly available access plans for AI resources.
Financial considerations	
• Financial resiliency and dependency on a third-party provider for AI services should be carefully considered. Reliance on start-ups has risks and benefits. • How wide should we open the door to health authority data with limited control? • Does the cost of developing AI solutions outweigh the actual and measurable benefits? Are we funding AI at the expense of other important types of traditional research?	• Engage legal experts (or those who write your agreements) early on, well before contracts are developed.
Education	
• There must be appropriate training of AI users in ethics, new scientific considerations, statistics, methods, etc. • We need to both engage and educate publics and patients who will eventually be the recipients of AI in relation to their healthcare. They will need to trust the outcomes of this research and we need to make sure this work is in alignment with their values and preferences.	• Create education and training materials for users of AI. • Conduct public engagement activities that also include educational components.
Research participant safety and care	
• Is AI used in research tested, reliable, etc? Does it pose any new risks to research participants? • How does AI impact the return of material incidental findings to participants?	• Ongoing support for and evaluation of AI research is essential. • Engage clinical users throughout the lifecycle of the AI initiative.

Theme	Recommendation
• Are there unintended consequences of employing AI in public health research (i.e., What happens if studies show that machine learning outperforms highly skilled professionals, for example, in disease detection?)	
Intellectual property	
• It is important for researchers to think carefully about the management and protection of their intellectual property (IP) when dealing with any novel technology and collaborations with others (including industry). • How are potential conflicts of interest, future commercial gains, and IP rights managed when the data is held by public entities?	• Engage with service providers within your organization early. Suggestions include: The Technology Development Office for PHSA researchers or the UBC University-Industry Liaison Office for those affiliated with UBC.
Governance	
• Legal as well as philosophical considerations (including liability and scope) with a learning autonomous algorithm. For example, what are the legal liability and moral consequences of producing a huge volume of results but potentially not being able to make sense of them or use them? • Marks the end of many traditional notions of privacy. We must be careful not to stretch concepts that are no longer relevant. We need to be nimble and adjust to new norms and standards. • How do we remain compliant from a regulatory perspective? Regulations and implementation guidance regarding research using AI are constantly evolving. • Who is accountable? What does it mean to have a privacy or security breach in this context? How do we respond, what is our recourse, how do we correct? How is our collective reputation impacted? • How does consent work with AI when you cannot explain what it is doing? • Are traditional notions of consent ethical or will they bias the data? Should waivers of consent be granted to maintain the integrity of the full dataset? • We need to ensure that we deal with the data appropriately based on trust relationships and between trusted organizations. Auditing can play a role in establishing transparency and trust. • Is the traditional research ethics framework appropriate for AI research or should a public health ethics approach be adopted?[8]	• Privacy, legal, quality, ethics, and other service providers should conduct their own research about new and emerging issues related to AI in their fields to help develop new approaches and processes. • Conduct quality improvement projects on AI initiatives already underway and share results widely with other organizations. • Instead of consenting to tools or a set of known research questions, we must move to a consent to good governance model and embrace principles of broad consent as outlined in the most recent proposed changes to the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS 2 (2018)*.

Final thoughts

AI has the potential to pose a range of systemic risks to organizations and often projects need to be reviewed on a case-by-case basis. Managing AI risks requires a systemic, multi-disciplinary approach underscored by an organization-wide, future proof strategy. Like all health research strategies, it should always be guided by the best interests of the patients we all serve.

Questions?

Please reach out to Holly Longstaff, Director of Research Privacy at PHSA holly.longstaff@phsa.ca if you have any questions about this Guidance. Please note that our Working Group does not endorse, review, or approve new projects or replace or replicate services provided within any BC Health Authority. We are simply available to support research privacy discussions around the implementation of novel technologies within our Health Authorities.

[8] BCCDC Ethics Framework and Decision Making Guide (2011) http://www.bccdc.ca/resource-gallery/Documents/Guidelines%20and%20Forms/Guidelines%20and%20Manuals/BCCDC_Ethics_Framework_Decision_Making_Guide.pdf