College of Registered Nurses of Manitoba

Artificial Intelligence (AI) in Registered Nursing Practice

Practice Support

Questions?

Contact Quality Practice:

204-774-3477 ext 301
1-800-665-2027 ext 301
practice@crnm.mb.ca

Date Published:

10/25

Date Reviewed:

N/A

Purpose

The purpose of the Artificial Intelligence (AI) in Registered Nursing practice support document is to provide registrants with background information about AI technologies that will support their practice as these tools are adopted, implemented, and evaluated. It also aims to alert registrants to some of the potential risks associated with emerging and established AI technologies and to offer strategies to help mitigate these risks.

Background

AI refers to a suite of computer systems that are designed to act in ways that resemble human intelligence, such as making decisions, solving problems, reasoning through information, and learning from experience.

It operates by recognizing patterns in large volumes of information and then using those patterns to make predictions, identify items, or offer suggestions. AI tools use diverse sources of data, including data used to help "train" pattern recognition.

There are different types of AI. For example:

- **Machine Learning**: A type of AI where computers learn from data and get better at making predictions or decisions without being directly programmed. For example, machine learning may analyze data to identify clients at risk for deterioration or support clinical decision-making.
- **Generative AI:** A kind of machine learning that creates new things like text, pictures, videos, or code by finding patterns in data. In healthcare, it can develop patient education materials or generate clinical notes from conversations.
- **Natural Language Processing**: AI that assists computers in understanding and processing human language. It can act as a medical scribe, translate patient instructions, or support chatbots that answer health-related questions.
- **Computer Vision:** Is a type of AI that allows computers to "see" and interpret images or videos, similar to humans. For example, it is used to analyze medical images and observe patient movement within a room.

Area of Use	Task	AI Tool Application Examples
Administrative Use	Scribes	Listen to meetings or clinical interactions to document and summarize what was discussed in meeting minutes or a health record entry.
	Summarizing	Review and summarize large amounts of data to facilitate easier review.
	Copywriting and drafting	Create written, audio, or visual material.
	Proofreading and editing	Proofread or edit drafts of publications.
Analytical Use	Research design, analysis, and prediction/modelling	Assist researchers by improving research design, or analyzing datasets for trends, patterns, outliers, or other characteristics.
	Optimizing workflows	Analyze and improve workflows in areas where registrants provide care.

Clinical Use	Diagnosis	Help clinicians diagnose health concerns by collecting and analyzing health data or diagnostic images.
	Triage	Assist clinicians in prioritizing client care by analyzing health data.
	Treatment planning, monitoring, and follow-up	Assist clinicians in developing care plans and monitoring various metrics that may inform reassessment and evaluation.
	Client teaching	Support clinicians in educating their clients.

Risk Considerations and Mitigation Strategies

To safely adopt and engage with AI technologies, registrants must carefully evaluate the associated risks. This section outlines several currently known risks that should be considered and provides suggestions for how registrants can mitigate them. Remember that, like any emerging technology, the known risks and recommended mitigation strategies will evolve over time. Any registrant using or contemplating the use of AI technologies should regularly reassess and adjust their practices to ensure the safety of their clients and colleagues.

Risk 1: Outputs of AI tools may not be reliable.

AI tools create information by first being trained on large datasets, which may come from public or private sources. That data is not always accurate or reliable, so the information produced by the AI can sometimes reflect the same mistakes or biases found in the data. AI processes what it has learned using techniques such as pattern recognition and language understanding, then generates an output intended to be helpful to the user.

Because the quality of the output depends on the quality of the data used for AI training, it's important to approach AI results with caution and critical thinking because the registrant is ultimately accountable and responsible for their actions and decision-making. The following are some of the reliability risks of using AI.

- **Bias:** If the data used to train AI is biased, it will produce biased results, which could negatively affect the information provided and, in turn, the care of the client.
  Example: A registrant relies on an AI tool that was trained almost exclusively on data from white male clients to diagnose a black female client's symptoms.
- **Errors and Overconfidence:** AI tools will learn from any errors in the source data. These errors can compromise the accuracy and validity of the output. The way questions are asked when using an AI tool can generate different responses. Finally, an AI tool may respond in a way that communicates a higher degree of confidence than is warranted.
  Example: A client's diet, exercise, and blood sugar logs are analyzed by an AI tool to create a plan of care. Unfortunately, the diet and blood sugar readings were not accurately tracked, so the care plan developed by the AI tool is flawed.
- **Hallucinations:** Defective AI training data or logic can lead the AI tool to spot incorrect patterns or make inaccurate predictions by 'filling in gaps.' This can result in inaccuracies, false positives, or false negatives in the output of an AI tool.
  Example: A registrant uses AI to create a discharge resource, but upon review, finds that some of the listed local support organizations do not exist.

- **Misinformation and Disinformation:** AI tools are trained on source data that may contain misinformation, disinformation, or content that is not evidence-informed. This can reduce the accuracy and reliability of the results.
  Example: A registrant asks an AI tool to describe the side effects of a vaccine. Unfortunately, the AI tool was trained on source data where vaccine misinformation is prevalent, resulting in a harmfully inaccurate output.
- **Deep Fakes:** AI deepfakes are media such as images, videos, or audio that are generated or altered using AI to mimic real people or events convincingly. Deepfakes can impersonate healthcare professionals to access client information, mislead clients by giving false information, or manipulate images or test results, leading to incorrect care plans.

Reliability risk mitigation strategies:

- **Human Oversight:** While, in some cases, it may be appropriate to use AI tools to automate low-risk administrative processes, human oversight should be incorporated into any workflow involving an aspect of AI. Any outputs that will impact a client's health care, care plan, or health record must be reviewed by a competent registrant.

  AI tools are an adjunct to, not a replacement for nursing knowledge, skill, or judgment. Policies and workflows should always require human oversight to verify the accuracy and reasonability of AI outputs.
- **Vigilant Critical Thinking and Clinical Judgment:** Any output of an AI tool should be thoroughly reviewed using critical thinking and clinical judgment for the presence of bias, mis/disinformation, errors, hallucinations, and deepfakes.
- **Use of Diverse and Accurate Data Sources:** Before using an AI tool in clinical or analytical practices, understand the source data it was trained on. Consider what data the AI can and cannot access, particularly being mindful of potential biases, especially those affecting minority or under-researched populations. When possible, use tools trained on large, diverse datasets.

  Consider that AI tools that are trained on error-prone data are likely to be inaccurate. Compare AI outputs with reputable, peer-reviewed, and current sources, where possible.

Risk 2: The use of AI tools may compromise client privacy and confidentiality.

Before entering personal health information or other identifiable client information into an AI tool, it is essential to understand how and where that data will be collected, stored, secured, used, and disposed of. The following are the privacy and confidentiality risks of using an AI tool.

- **Collection and Storage:** When data is entered into AI tools, it is stored on servers. These servers may be located outside of Canada and subject to different laws regarding the access and sharing of data.
- **Security:** While some AI tools will have protections in place to secure data, these protections are not uniform, perfectly secure, or error-proof. Who will have access to the data entered into the AI tool, and how it is reviewed or audited, will vary.
- **Use/Disclosure:** How the data is used and to whom it will be disclosed can vary. In some cases, data entered into an AI tool may be used to train the tool for other purposes and might, at some point in the future, be improperly disclosed to others. Many available AI tools offer users the ability to adjust settings to control how their data is used, but this will differ depending on the tool.
- **Destruction:** AI tools often claim that users can delete their input data or clear their history. However, how these functions occur can vary significantly, and in some cases, it may not be possible to ensure that any data is ever fully destroyed.

Privacy and confidentiality risk mitigation strategies:

- **Privacy Impact Assessment:** Before entering confidential or sensitive health information into an AI tool, ensure a privacy impact assessment has been completed for that tool, for the intended practice setting and use. Most practice settings have approved administrative processes to ensure these assessments are performed properly.
- **Informed Consent:** Ensure that clients provide informed consent for the use of any AI tool in their care. This may involve teaching the client about the risks, benefits, alternatives, as well as information on how their health information will be collected, used, disclosed, and destroyed. Practice setting policies should inform where, when and how AI-informed consent is obtained, and documented.
- **Understanding AI Regulation:** Familiarize yourself with any laws (municipal, provincial or federal), College practice expectations, and employer policies related to the protection of sensitive, confidential, or personal health information and consider if the use of a proposed AI tool would comply with those expectations.
- **AI Tool Settings:** Ensure that any privacy, security settings are properly configured to protect the security and confidentiality of your data.
- **Stay Informed of Updates:** Keep apprised of AI tool changes to confidentiality or data security, as well as updates that could affect current protections.
- **Managing Breaches:** Take action to manage and report any actual or potential data security or privacy breaches brought to your attention using appropriate channels.

Risk 3: Advancements in AI technology may outpace or replace registrants' competency.

AI tools have the potential to improve the efficiency and quality of healthcare. Developing, adopting, and implementing the use of AI tools will challenge the knowledge, skill, and judgment requirements of registrants.

The following are the competency risks of using AI.

- **Skill Development:** The rise of new AI tools and the need for skills in managing technology may affect whether they are adopted in practice, possibly creating a gap in who can use them effectively.
- **Administration and Governance:** Laws, employer policies, or regulator practice directions may not keep up with technology, leading to potential gaps and risks that the registrant must manage themselves.
- **Overreliance on AI Causing Competency Degradation:** The ease and access of many AI tools may result in an eventual reliance on AI tools, which can contribute to the loss of knowledge, skill, judgment, and critical thinking in the nursing profession. In the absence or access to AI tools, the registrant must be able to depend on their competence, experience, and critical thinking to provide safe client care.

Competency risk mitigation strategies:

- **Reflection:** Regularly, consider "If the AI tool stopped working today, would I still be able to provide safe, quality nursing care?" If there is doubt, consider what learning or practice safeguards are necessary to ensure competency in registered nursing practice is maintained.

- **Professional Development:** Participate in learning activities regarding ethical, legal, and professional expectations when using AI tools. Make efforts to improve competence with AI tools that are being adopted in healthcare and their practice setting. Identify learning needs related to technological literacy and seek out resources to help fill any gaps in knowledge, skills, or judgment.
- **Collaboration:** Participate in discussions and ask questions within your practice setting about the safe and appropriate integration of AI tools. Identify subject matter experts, such as privacy officers or information technology supports, who could assist in answering any questions about AI tools.

Risk 4: The adoption of AI tools risks dehumanizing the client experience.

Clients benefit from client-centeredness, compassion, empathy, and dignity. Professional registered nursing relies on and values human connection and the therapeutic relationship as foundational tools for providing quality care. AI tools, such as AI chatbots and AI-client surveillance technology, may improve access to scarce human resources, standardize care, and enhance efficiency; however, the adoption of AI tools, particularly those designed to replace or reduce the interaction between care providers and clients, risks dehumanizing the client's experience.

Risk mitigation strategies:

- **Reflect:** Registrants should reflect early and often about how AI tools impact the client experience and their ability to establish a therapeutic relationship. Registrants should critically consider what is gained and potentially lost by adopting AI technology.
- **Advocate:** When decisions are being made about the use of AI with clients, registrants should advocate for nurses, clients, and their families to be involved in those decisions. Registrants should respectfully advocate for a careful, balanced, and client-centered evaluation of these tools before implementation.
- **Educate:** When AI interfaces with the client directly, registrants should provide education to clients about the technology, its benefits, and its risks and elicit feedback from them about their experience.
- **Offset Loss:** Identify which aspects of client or colleague interactions may be diminished by introducing AI technology and proactively adopt alternative meaningful methods to sustain relationships.

AI technologies are rapidly evolving, and information may change quickly due to new research and regulations. This document serves as a guide for users at the time of publication. Registrants are encouraged to stay informed and check back for updates regularly.

Glossary

AI Training - is the process of teaching a computer program how to recognize patterns and make decisions by showing it lots of examples. Over time, the AI "learns" from these examples so it can make predictions or generate answers when given new information.

Chatbot - is a computer program that uses AI to simulate conversation with people. It can answer questions, provide information, or assist with tasks by interpreting text or voice input and giving a response.

Deep Fakes – are media, such as images, videos, or audio, that are generated or altered using AI to mimic real people or events, convincingly but falsely showing people saying or doing things that never happened.

Hallucinations - is when an AI tool generates information that appears plausible but is false, misleading, or nonsensical.

Privacy Impact Assessment (PIA) – a PIA is a process that an organization can use to identify and address potential privacy risks when contemplating a new, or evaluating an existing, program, service or activity. The PIA process examines potential impacts to privacy and considers reasonable measures to lessen these impacts.

Glossary

Ramírez-Baraldes, E., García-Gutiérrez, D., & García-Salido, C. (2025). Artificial intelligence in nursing: New opportunities and challenges. European Journal of Education. https://onlinelibrary.wiley.com/doi/am-pdf/10.1111/ejed.70033

Healthcare Excellence Canada. (2021, November). Implementing artificial intelligence in Canadian healthcare. https://www.healthcareexcellence.ca/media/qdmn0p3b/20211208_aireport_en.pdf

Healthcare Information and Management Systems Society. (2023). 5 rights of AI in healthcare. https://cdn.sanity.io/files/sqo8bpt9/

Healthcare Insurance Reciprocal of Canada. (2020, August). Artificial intelligence: A guide for healthcare administrators and risk managers. https://www.hiroc.com/system/files/resource/files/2020-10/Artificial%20Intelligence%20-%20Risk%20Management%20in%20Healthcare_2.pdf

Rony, M.K.K., Parvin, M.R., & Ferdousi S. (2023). Advancing nursing practice with artificial intelligence: Enhancing preparedness for the future. Nursing Open. https://pmc.ncbi.nlm.nih.gov/articles/PMC10733565/

References

Australian Health Practitioner Regulation Agency. (2024, August 22). Further information about AI: What is artificial intelligence? https://www.ahpra.gov.au/Resources/Artificial-Intelligence-in-healthcare/Further-information-about-AI.aspx#

IBM. (2023). What are AI hallucinations? https://www.ibm.com/think/topics/ai-hallucinations

Manitoba Health. (2025, October 1). The Personal Health Information Act (PHIA). https://web2.gov.mb.ca/laws/statutes/ccsm/p033-5.php?lang=en

Manitoba Ombudsman. (2015, September). Privacy impact assessment tool. https://www.ombudsman.mb.ca/wp-content/uploads/2025/03/pia-tool-web.pdf

Navarro, M.O., Fernández-García, D., Cuartero, M.N., & Forero-Rincón, O. (2024). Possible health benefits and risks of deepfake videos: A qualitative study in nursing students. Nursing Reports. https://pmc.ncbi.nlm.nih.gov/articles/PMC11503397/

College of
Registered Nurses
of Manitoba

210 Commerce Drive
Winnipeg, Manitoba R3P 2W1
204-774-3477
www.crnm.mb.ca