

CRIC Guiding Principles for AI use in Market Research

Introduction

The purpose of these guiding principles is to provide a framework for the use of Artificial Intelligence¹ (AI) in market research, given the increasing implementation and use of AI. The aim is to ensure the strategic, ethical and responsible use of AI applications.

Since its release in 2024, the framework has served its intended purpose of providing practical guidance that balances innovation with responsibility. The CRIC AI Ethics Sub-committee has now added addendums to several sections with the purpose of strengthening rather than fundamentally changing them.

Guiding Principles

1. **Transparency:** Ensure transparency and accountability in the use of AI. Any organization using AI should have open and clear communication with clients, respondents, and the general public about any AI integration into processes, explaining how, why and when AI is used.

Transparency Addendum

Organizations should distinguish between insights solely derived from AI and those generated through human analysis (assisted by AI or otherwise). This includes:

- Explaining the role of AI in fieldwork (including the use of Synthetic Personas² and the role of AI in data cleaning), analysis and report generation processes (e.g., preliminary data sorting, pattern identification, theme extraction, report generation)
- Clearly specifying if Synthetic Data³ was used and the extent to which it was used
- Providing context about how human oversight was applied to verify or refine AI-generated content and insights
- Identifying limitations of AI-derived content and insights

2. **Data security:** Use of AI applications could raise data security considerations. Ensure adherence to relevant CRIC standards, essential security practices in the CRIC Information Security Toolkit, and client contracts in terms of data transmission, storage and security. Researchers should pay particular attention to how information entered into AI applications will be used by the application for data learning and/or the production of other output. In situations where multiple standards or contracts may apply, the one that sets the highest bar for data security should be the guiding document.

Data Security Addendum

Security Monitoring and Risk Management

- Organizations should establish ongoing monitoring systems to ensure AI security resilience, including:
 - Conduct regular security audits that include identifying risks related to the use of AI
 - Ensure incident response procedures address AI related security breaches

Third-Party AI Integration

When incorporating external AI applications, organizations should maintain rigorous security standards:

- Conduct due diligence and regularly review third-party AI providers' security policies and compliance status
- Establish and document secure data transmission protocols between research systems and external AI applications

3. Protecting participants (data subjects) from harm: As with all research tools, adhere to the principles of a strong privacy management program as required by the CRIC Standards and outlined in the CRIC Privacy Toolkit when using AI. Ensure any data and inputs used by AI applications are lawfully collected, used, and disclosed, taking account of applicable privacy and respondent rights to understand how their data is being captured and stored. Specifically, data subjects must be clearly notified of the use of Synthetic Persona for data collection at the beginning of the research. It is essential to clearly inform participants when they are interacting with an AI application and not a human being.

Protecting Participants from Harm Addendum

AI-Mediated Interaction, Participant Autonomy, and Well-Being

When AI applications are used in direct or indirect interaction with research participants - such as Synthetic Personas, including AI moderators, chatbots, adaptive questioning systems, or automated prompting - organizations should take additional steps to safeguard participant autonomy, well-being, and dignity.

Specifically:

- **Participant Awareness and Expectations**
Participants should be provided with clear, accessible information about the nature of AI-mediated interactions, including the capabilities and limitations of the AI system. AI applications should not be presented in ways that could reasonably mislead participants

into believing they are interacting with a human being or that the system possesses human understanding, judgment, or empathy.

- **Limits on AI Autonomy in Sensitive Contexts**

The use of AI-mediated interaction should be carefully evaluated in research involving sensitive, personal, or emotionally charged topics. Where there is an increased risk of distress or misunderstanding, organizations should implement safeguards such as human oversight, escalation protocols, or restrictions on fully autonomous AI interaction.

- **Participant Control and Choice**

Where feasible, participants should be offered clear options regarding their participation in AI-mediated research, including the ability to opt out of AI interaction or request human involvement without penalty or disadvantage.

- **Prevention of Experiential Harm**

AI systems should be monitored to reduce the risk of participant harm arising from inappropriate tone, misinterpretation of responses, repetitive or intrusive questioning, or unintended reinforcement of sensitive content. Outputs generated by AI that directly affect the participant experience should be subject to review and refinement.

- **Accountability and Redress**

Organizations remain fully responsible for participant experiences and outcomes when AI is used. Clear processes should be in place to address participant concerns, complaints, or adverse events arising from AI-mediated research interactions.

4. **Work to minimize biases:** Understand and monitor the potential biases of AI and prioritize the needs of individuals and communities, including equity-deserving groups. Researchers must remain vigilant about the inherent biases and limitations of AI, taking steps to minimize their impact while fostering accountability. Evaluate the outputs of AI applications, including generative tools, to minimize biases and inaccuracies. In addition, when content is predominantly or entirely generated by AI, it should be explicitly identified as such to maintain transparency. This ensures that clients are fully aware of the source and method of content creation.

5. **Ensure oversight:** CRIC members should ensure effective monitoring is in place and are encouraged to conduct regular bias audits of their AI applications, create test environments, and establish human oversight mechanisms for AI applications to ensure accountability. Teams should be multidisciplinary, including data scientists, ethicists, and legal experts to ensure a comprehensive understanding.

Ensure Oversight Addendum

Organizations should extend existing research ethics processes to explicitly incorporate AI-related considerations, ensuring that AI governance is aligned with the same level of rigour applied to traditional research ethics. This includes:

- Leveraging established research ethics frameworks, including risk identification, assessment of impacts on participants and the public, clarification of roles and accountability, and review by relevant ethics or governance committees. Integrate AI-specific considerations such as bias, transparency requirements and data security obligations into these frameworks.
- Ensuring that AI-enabled projects undergo ethical review proportional to their scope, risk, and potential impact, maintaining alignment with Canadian research ethics principles and CRIC Standards.

Definitions

1. **Artificial intelligence:** set of technologies that are designed to simulate human intelligence and to provide problem-solving capabilities (this would include Large Language Models/LLMs)
2. **Synthetic data:** means information that has been generated to replicate the characteristics of real-world data.
3. **Synthetic persona:** means a digital representation of a person generated to mimic the behaviours, preferences, and characteristics of real people or groups.