Guidelines for Ethical and Secure Use of AI-Based Software in Research

TEACHERS COLLEGE INSTITUTIONAL REVIEW BOARD

Purpose

This guideline provides researchers with clear expectations and procedures for using AI-based software in studies involving human subjects. It is essential to ensure the ethical, secure, and compliant use of AI tools in line with institutional policies and federal regulations.

While TC Information Security (TCIT) evaluates the technical and data security risks of AI-based software, TC IRB evaluates its ethical implications and compliance with human subjects protections. Depending on the nature of the software and data involved, both reviews may be required.

Early Consultation with TCIT

Any researcher interested in using AI-based software for a proposed study should reach out to TCIT first.

Inform TCIT of the AI features you plan to utilize, including potential risks and concerns surrounding data security, privacy, and user information.

Undergo a Security Assessment

AI-based software requires a security assessment to ensure it aligns with the institution's data protection policies, including whether it is IRB compliant. This assessment is essential for ensuring that the app or software does not compromise research data or violate privacy regulations.

Inform TCIT of the specific AI functionalities you plan to use and provide a summary of associated risks. These risks may include, but are not limited to:

- □ Potential for unauthorized access, data leaks, or breaches involving sensitive or personally identifiable information (PII).
- □ AI tools may collect or process data in ways that are not transparent or exceed the original scope of consent provided by participants.
- □ Many AI-based software, especially free versions, may store data on external servers or share it with third parties for analytics or advertising purposes.
- □ AI algorithms may reflect or amplify bias, especially if trained on unrepresentative data. This may affect participant inclusion or skew research findings.
- □ Some tools operate as "black boxes," making it difficult to audit how decisions or outputs are generated.

Early identification of these risks helps ensure that appropriate safeguards, approvals, and informed consent processes are in place before research initiation.

Understand the Case-by-Case Approval Process

Each AI-based software will undergo an individual approval process. The TCIT team will evaluate its security measures, privacy policies, and data-handling practices.

Note: Approval is not automatic and may take time. Please consider the processing time when submitting for approval. Every app is to be evaluated based on its specific features and risks.

Free Software Vs. Paid Software Considerations

When submitting software for a security assessment, keep in mind that paid versions of software will likely be approved over free versions due to differences in AI data security and storage policies:

- **Free Software**: Often, free AI tools collect, store, or even share/sell user data to fund their operations in exchange for free access. This makes such a version inherently more risky for use in research.
- **Paid Software**: While paid software is generally more secure and less likely to share user data, it still requires approval. Data security concerns must still be addressed.

Due Diligence on Software Terms of Use and Privacy Policies

Researchers should carefully read the terms of service, privacy policies, and data usage agreements of the AI-based software before use. Make sure to understand the following key aspects:

- **Data collection:** What data is being collected, and how is it stored?
- **Data Sharing:** Is data shared with third parties or used for purposes other than the scope of the research?
- **Retention and Deletion:** How long will your data be stored, and how can it be deleted if necessary?

Maintain Records and Documentation

Researchers must keep detailed records of:

- Security assessments conducted by TCIT
- Correspondence or documentation of approval
- Versioning and software updates

This documentation may be required during IRB review or compliance audits.

Ensure Ongoing Compliance

AI-based software and institutional policies evolve rapidly. Researchers must:

- Monitor for updates to the software's privacy or data handling policies
- Reassess risks if the tool's use in the study changes
- Notify TCIT and the IRB if any software is revoked or significantly modified

Example: Otter.AI is in the "Reviewed but Not Approved for General Use" category, which means significant issues were identified that could impact a user's ability to interact with and use the product effectively. It is strongly recommended that you identify a more accessible application approved for use at TC. Continued use of revoked tools is prohibited.

Generative AI Use and Research Ethics

If using generative AI (e.g., ChatGPT, DALL·E) to create content (such as interview questions, surveys, or summaries), researchers must:

- Disclose this use in their IRB application
- Validate the output for accuracy and ethical alignment
- Clarify authorship and data ownership where relevant

Researcher Checklist Before Using AI-Based Software

- □ Consult with TCIT about the software and its features
- □ Submit software for security review and risk assessment to TCIT
- □ Review and understand the Terms of Use and Privacy Policy of the software
- □ Disclose the use of AI in the IRB application and the consent document (s) as applicable
- □ Maintain documentation of approvals and communications with TCIT and TC IRB
- □ Monitor for TC policy or software updates during the study.

Frequently Asked Questions (FAQ)

Q1: Can I use ChatGPT to draft consent forms, interview questions, or recruitment materials?
A: Yes, but you must disclose this use in your IRB application. You are responsible for verifying the accuracy, appropriateness, and ethical implications of all AI-generated content.

Q2: Does AI software used only for transcription (e.g., Otter.ai) need approval?
A: Yes. Any AI-based software processing human subjects data (even transcription) must undergo a security assessment by TCIT, regardless of its function.

Q3: If the AI tool only processes de-identified data, do I still need IRB or TCIT review?
A: Possibly. While de-identification reduces some risks, you must still consult TCIT for a security assessment. The IRB will evaluate whether the data truly meets de-identification standards.

Q4: Can I switch from a free version to a paid version of the same software during the study?
A: Yes, but you must notify TCIT and the IRB. Changes in software versions—especially from paid to free—can result in differences in data security, privacy protections, and feature access, which may compromise participant confidentiality or study integrity. If a paid subscription is expected to expire during the course of the study, you should either:

- Plan in advance to renew the subscription, or
- Reassess the use of the software for the study altogether.

All changes in tools used for research purposes should be documented. Depending on the scope of the change, TCIT and/or TC IRB notification or approval may be required.

Q5: What if the AI tool I plan to use gets revoked after my study begins?
A: You must immediately stop using the tool and notify both TCIT and the IRB. Continuing to use a revoked application could jeopardize data security and regulatory compliance.

Special Considerations for Qualitative Research Using AI-Based Software

AI technologies are increasingly used in qualitative research workflows, such as transcription, coding, analysis, and content generation. While these tools can improve efficiency, they introduce unique ethical, security, and methodological challenges when working with narrative, sensitive, or participant-derived data.

Researchers conducting qualitative research using AI tools must:

Guidelines for Ethical and Secure Use of AI-Based Software in Research

TEACHERS COLLEGE INSTITUTIONAL REVIEW BOARD

1. **Protect Participant Voice and Narrative Integrity**
   - Participant narratives are identifiable even when direct identifiers are removed.
     - AI-based transcription, summarization, or coding software may inadvertently expose sensitive information.
     - Narrative reconstruction or misinterpretation by AI must be considered a risk to data integrity.
   - Researchers must validate AI outputs against original transcripts or recordings to avoid misrepresentation or loss of nuance.

2. **Disclose AI Use Clearly**
   - If AI is used in any stage (e.g., transcription, thematic coding, data visualization), this must be disclosed to:
     - The IRB,
     - Participants (through informed consent forms),
     - And in publications or presentations resulting from the research.

   Sample disclosure in the Consent Form:

   > *"Automated tools may assist with transcription, analysis, or organization of interview content. However, your responses will not be publicly shared, and human review will ensure accuracy."*

3. **Vet AI Tools for Cultural and Contextual Sensitivity**
   - Many AI models are trained on generalized, Western-centric datasets and may misinterpret:
     - Non-Western cultural references,
     - Linguistic nuances,
     - Gender, disability, racial, or ethnic identifiers.
   - Researchers should critically review AI-coded themes or summaries for cultural misrepresentations or biases.

4. **Manage Data Security During Qualitative Analysis**
   - AI-based coding or analysis software often requires uploading full transcripts or audio recordings to external servers.
   - Any tool used must first pass a TCIT security assessment, even if only "de-identified" data is processed.
   - Researchers must also:
     - Ensure transcripts are stored in secure, TC-approved systems.
     - Prevent storage on consumer-grade or non-secure cloud platforms unless explicitly approved.

5. **Maintain Human Oversight**
   - AI should not replace human judgment in qualitative analysis.
   - The final coding, thematic development, and interpretation must be reviewed and validated by the research team to ensure ethical integrity and methodological rigor.

Other Questions?

- **Contact TCIT Information Security** (tcit@tc.edu) early to avoid approval delays.
    - Check the real-time availability of TC-approved software, including AI-based tools, by visiting the TCIT Available Software page.
- **Contact the IRB Office** (irb@tc.edu) if your use of AI changes or if issues arise during proposal review.