TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER

Operating Policy and Procedure

HSC OP: 52.21, Acceptable Use of Artificial Intelligence (AI) Tools

PURPOSE: The purpose of this Health Sciences Center Operating Policy and Procedure (HSC OP) is to establish clear expectations and guidelines for the responsible, ethical, and compliant use of artificial intelligence (AI) tools within Texas Tech University Health Sciences Center's (TTUHSC). As AI technologies are increasingly integrated into education, research, clinical care, and administrative functions, it is essential to ensure their use aligns with institutional values, protects sensitive information, complies with applicable laws and regulations, and supports the integrity of academic, clinical, research and business operations.

REVIEW: This OP will be reviewed by March 1 of each odd-numbered year (ONY) by the Chief Information Officer and the Chief Compliance Officer, with substantive revisions forwarded to the AI Governance and Risk Committee and People and Operations Council.

DEFINITIONS: For purposes of this policy, the following term is defined as follows:

Artificial Intelligence (AI) Tools are defined as software, systems, or applications that use machine learning (ML), natural language processing, large language models, computer vision, or other algorithmic techniques to perform tasks that typically require human intelligence. These tasks may include, but are not limited to, generating or analyzing text, images, audio, or video; making predictions or recommendations; identifying patterns; or assisting with decision-making.

Examples of AI tools include (but are not limited to): generative AI platforms (e.g., large language model chatbots), automated translation services, image or voice recognition systems, predictive analytics tools, and clinical decision support systems.

Exclusions (What is not an AI tool for this policy):
The following are not considered AI tools under this policy unless they incorporate AI/ML features as described above:

- Basic deterministic utilities (e.g., calculators, basic rule-based spell/grammar checkers, simple macros, mail-merge).
- Traditional business software without AI/ML components (e.g., word processors, spreadsheets, presentation applications).
- Simple automation or workflow tools that execute fixed rules (e.g., if-this-then-that scripts, scheduled batch jobs).
- Embedded device features that do not use AI/ML (e.g., basic camera auto-focus, template OCR with fixed rules).

Boundary cases:
- If a product or feature advertises or includes "AI," "smart," "assist," "predictive," or similar capabilities (for example: predictive text, generative writing, image synthesis, ML-based analytics), those capabilities are in scope even if the larger product would otherwise be excluded.
- Vendor updates that add AI capabilities bring that product or feature into scope on the effective date of the update.
- When in doubt, treat the feature as an AI tool for the purposes of this policy and consult the AI Governance & Risk Committee for a formal determination.

POLICY/PROCEDURE:

With the increasing integration of AI tools into university activities, it's essential to use these technologies responsibly.

1. Guiding Principles

These principles guide responsible adoption, development, procurement, and everyday use of AI tools at TTUHSC. They apply across education, research, clinical care, and administrative domains and should inform decisions, procedures, and trainings.

a. Transparency
AI use must be disclosed and documented appropriately. Users are responsible for communicating when content, recommendations, or analysis is produced or significantly influenced by AI. Documentation should include the type of AI tool used, its purpose, and any limitations or assumptions inherent in its output. Transparency also includes providing sufficient information for stakeholders to understand how AI contributes to decisions or content.

b. Accountability
Human users have final responsibility for all decisions and outcomes resulting from AI use. This includes ensuring compliance with institutional policies, professional standards, and legal obligations. Users must evaluate AI outputs, recognize the tool's limitations, and take corrective action if AI-generated results are inaccurate, misleading, or inappropriate. Accountability also involves documenting decisions made with AI tools to maintain traceability.

c. Fairness & Integrity
AI tools must be used in ways that uphold fair treatment of all individuals and avoid discrimination. Users are responsible for identifying, assessing, and mitigating instances where AI outputs may lead to unfair or harmful impacts—especially in situations that affect groups with higher risk of adverse outcomes. This responsibility also includes careful review of training data, models, and applications to ensure they do not reinforce disparities.

d. Privacy & Security
AI use must protect sensitive, confidential, and personally identifiable information. Users must comply with applicable laws, regulations, and institutional policies regarding data privacy and security. Data input into AI systems should be minimized to only what is necessary for the task, and secure handling, storage, and transmission practices must be followed to prevent unauthorized access or breaches.

e. Human Supervision
AI is intended as a decision-support tool, not a replacement for human judgment. All outputs must be subject to human review, with the capacity to override or modify AI-generated recommendations. This is particularly critical in academic, research, clinical, and other high-risk settings where decisions have significant consequences. Supervision also includes continuous monitoring of AI performance to ensure it aligns with institutional values.

2. AI Governance Structure

a. The AI Governance and Risk Committee is established by the President's Cabinet to provide strategic and operational oversight for all AI-related activities, ensuring alignment with institutional mission, regulatory compliance, ethical standards, and risk management.

b. The AI Governance and Risk Committee may include the following representatives:
- Chief Compliance Officer (Co-Chair)
- Chief Information Officer (Co-Chair)

- Clinical Affairs Representative
- Provost or Academic Affairs Representative
- Research Compliance Representative
- Institutional Privacy Officer
- Information Security Officer
- Purchasing/Contracting Representative
- Human Resources Representative
- General Counsel Representative
- Ethics Representative
- Faculty and Student Representatives (optional)
- Subject-matter AI/ML experts (ad hoc or permanent)

c. The AI Governance and Risk Committee shall have the following responsibilities:
   - Approve and maintain AI policies, procedures, and standards.
   - Review and approve proposed AI tools and high-risk projects across clinical, research, education, and administrative domains.
   - Assess risk, including privacy, security, bias, and ethical considerations.
   - Monitor AI system performance and compliance post-deployment.
   - Evaluate vendor partnerships and contracts for AI solutions.
   - Oversee training programs and competency requirements for AI users.
   - Receive and review reports of incidents or concerns; recommend mitigation and corrective actions.

3. Allowable Use

In accordance with HSC OP 56.04, Data Security and Privacy, all TTUHSC-owned data is classified into four types based on its privacy and security level: Public Data, Sensitive Data, Confidential Data, and Regulated Data. The type of data significantly affects how users can use it with AI tools, because of privacy, security, legal, and ethical considerations.

a. Public Data may be used freely with AI tools for generating insights, summaries, or training (unless the platform restricts it).
b. Sensitive, Controlled, and Regulated Data can be used with AI tools that are managed by TTUHSC and covered by contracts explicitly protecting TTUHSC data. These contracts should ensure that the data is not utilized for training models or is isolated in a separate instance inaccessible to external parties.

AI tools should be used as decision-support tools and not as decision- making tools. In all cases, use should be consistent with the HSC OP 52.09, Confidential Information and HSC OP 56.01, Acceptable Use of Information Technology Resources. Users may use only the information and information systems to which they have been given authorized access. Anyone who has access to confidential information regarding TTUHSC employees, Students, patients, affiliates, or any other information made confidential by TTUHSC policies or law will take reasonable and necessary steps to maintain the confidentiality and privacy of such information.

4. Prohibited Use

a. Unauthorized AI Tools: AI tools that lack a TTUHSC contract and appropriate data-sharing safeguards are not approved for use with Sensitive, Controlled or Regulated Data.
b. Confidential Information: AI tools may not be used with personal, confidential, proprietary, or other sensitive information unless a contract explicitly ensures that TTUHSC data is protected from use in training models or is isolated in a secure environment inaccessible to external parties. This includes, but is not limited to, student records protected under FERPA, health information covered by HIPAA, proprietary data, and any other information classified as Confidential.
c. Non-Public Output: AI tools should not be used to generate outputs that would be considered non-public. Examples include but are not limited to generating proprietary or

unpublished research; legal analysis or advice; recruitment, personnel, or disciplinary decision making; completion of academic work in a manner not allowed by the instructor; creation of non-public instructional materials; and grading.

d. Fraudulent or Illegal Activities: AI tools must not be used for activities that are illegal, fraudulent, or violate any state or federal laws, or TTUHSC or TTU System policies.

5. Additional Guidance

a. Personal Liability: Be aware that accepting click-through agreements without delegated signature authority may result in personal responsibility for compliance with the terms and conditions of the AI tool.
b. Procuring AI Tools (including free tools): Contact TTUHSC IT before purchasing (or acquiring for free) AI tools or products that contain functions that rely on AI to operate – especially if TTUHSC resources or data will be used.
c. Avoid inputting Personal Information: Do not input Personal Information about TTUHSC employees, students, faculty, or other stakeholders into an AI tool unless explicitly allowed under validated contracts and security controls approved by TTUHSC IT and the Office of Institutional Compliance.
d. Respect intellectual Property (IP) and Contract Terms: Users must adhere to the terms and conditions of AI tools and protect intellectual property rights. Ensure that inputs and outputs comply with copyright, patent, data protection, and identity theft regulations. Many digital resources provided by TTUHSC Libraries are subject to vendor licenses that may restrict AI use. Contact the Libraries for guidance on acceptable use of licensed content with AI tools or large language models.
e. Verify AI Output Accuracy: Always confirm the accuracy of AI-generated information before relying on it. AI outputs may be inaccurate, biased, or fabricated (“hallucinations”) and may include copyrighted material. Users are responsible for any published content that incorporates AI-generated material.
f. Disclose AI Use: Clearly disclose when written materials or other work products are generated with or derived from AI tools. Transparency is required whenever AI outputs are used.
g. Respect Third-Party Intellectual Property: Do not present AI-generated outputs as your own. When quoting, paraphrasing, or borrowing ideas from AI outputs, ensure accuracy and avoid infringing on another party’s intellectual property rights.
h. Prohibit Malicious Use: Do not use AI tools to create malicious content, including malware, viruses, worms, or trojan horses, or to bypass TTUHSC or third-party network security controls.