DIR Code of Ethics (1 TAC §219.11(a))

(a) As required by Texas Government Code § 2054.702, state agencies and local governments shall adopt the AI Code of Ethics established by this section and follow the ethical principles included herein as they procure, develop, deploy, or use artificial intelligence systems.

(b) Preamble

(1) AI systems have the potential to transform the way our state and local governments serve Texans. AI systems can create efficiencies, support economic and scientific advancement, and improve the safety and well-being of our communities. The State of Texas supports the use of AI systems by governmental entities to improve the services they deliver to Texans and to lead in innovative AI adoption in the public sector.

(2) While they have significant potential value, AI systems also pose substantial risks if not implemented ethically and responsibly. AI risks vary based on the system involved, how it is used, and who uses it. AI systems are often trained on large amounts of data from a variety of sources, which can lead to inaccurate outputs. To the extent that AI systems are trained on or used to process PII, they may raise significant privacy concerns, particularly when the systems are deployed outside of a secure government environment. Malicious actors can utilize AI to develop more advanced cyberattacks, bypass security measures, and exploit vulnerabilities in systems. These and other AI risks make it a uniquely challenging technology for governmental entities to use safely, but with appropriate guardrails, governmental entities can limit the risks of AI and secure its many benefits for Texans.

(3) Governmental entities must limit the potential harm of AI systems by managing risk and prioritizing trustworthy and responsible development and deployment of AI consistent with the National Institute of Standards and Technology AI Risk Management Framework. Creating trustworthy AI requires balancing each of these principles based on the identified risks of an AI system and the context in which it is used.

(4) This section articulates the principles of ethical AI implementation that governmental entities must strive for when procuring, developing, designing, or using AI systems.

(c) Human Oversight and Control

(1) Human oversight plays a crucial role in ensuring that AI systems operate ethically. While AI can analyze vast amounts of data much faster--and sometimes more accurately--than humans, it lacks the human judgment necessary to ensure that its decisions align with societal values and the rights granted to individuals under the law. Ensuring human control over AI systems mitigates risks of inaccurate or undesirable outputs and allows for revision of the rules established during development of the system and to the data that supports the system's decision-making.

(2) Governmental entities:

(A) Must deploy AI systems in ways that enable humans to review and analyze inputs and outputs at appropriate intervals throughout the AI lifecycle;

(B) May incorporate a level of human oversight reasonably commensurate to the risks associated with a particular AI system, with heightened scrutiny AI systems requiring increased human oversight relative to lower risk systems; and

(C) Must ensure AI systems can be paused, restricted, or disabled until harmful or inaccurate decision making can be remedied.

(d) Fairness

(1) The data used to develop AI systems must adequately represent the subjects or people about which AI systems make judgments, decisions, or predictions. Incomplete or inaccurate data can result in unlawful harm.

(2) Governmental entities:

(A) Must ensure their use of AI systems does not infringe upon the legally protected rights and liberties of the individuals they serve or result in unlawful harm; and

(B) Must implement data governance practices for AI systems throughout the AI system's lifecycle to ensure fairness.

(e) Accuracy

(1) While AI systems are overall improving in their ability to deliver more accurate results, inaccurate outputs remain a significant risk when using AI systems.

(2) Governmental entities:

(A) Must train their employees to understand the importance of verifying AI outcomes for accuracy;

(B) Must formalize processes for monitoring system accuracy before the deployment of an AI system and throughout its life cycle, as a system's accuracy may change over time; and

(C) Shall, when feasible, implement processes to improve the accuracy of AI systems by training the systems using human feedback or improving retrieval-augmented generation by ensuring the accuracy and relevance of the underlying data used by the tool to develop answers.

(f) Redress

(1) Providing a method for redress will promote public trust in both the AI system and in the entity that deploys it.

(2) Governmental entities:

(A) Must provide a mechanism to seek redress for those impacted when an AI system makes a consequential decision that results in unlawful harm about their rights or access to governmental services;

(B) Must have a designated point of contact for individuals to address when seeking information about an unfair consequential decision; and

(C) Must develop internal procedures to allow employees to identify and remedy negative impacts caused by the use of AI systems.

(g) Transparency

(1) Establishing transparency for AI systems means providing information about the data, models, and outputs of an AI system to both the individuals interacting with the system and those deploying it. Strong transparency practices will build public trust in the AI systems governmental entities use.

(2) Governmental entities:

(A) Must collaborate with developers of AI systems and demand transparency to understand how a system operates, the source of the data the system was trained on, and its intended use cases;

(B) Must strive to understand the capabilities of the system and how it makes decisions;

(C) Must disclose when individuals interact with a public-facing AI system and when an AI system is used to make consequential decisions about their rights or access to governmental services; and

(D) Must never represent AI systems as human when interacting with the public.

(h) Data Privacy

(1) Governmental entities have a responsibility to protect the PII they collect and process about individuals, and both legal and ethical restrictions exist on what PII entities share with third parties. Data privacy principles likewise apply to the PII governmental entities process in and share with AI systems.

(2) The most effective method for protecting PII is through data minimization.

(3) Many AI systems rely on vast amounts of PII to make predictions and decisions. Sharing PII with an AI tool may violate privacy laws and obligations the entity has to the individual, particularly when using a tool outside the governmental entity's secure environment.

(4) Governmental entities:

(A) May collect and maintain only that PII needed for operations and must establish a process to delete PII consistent with records retention schedules and other legal requirements.

(B) Must strive to understand what PII the AI system uses, how that PII has been and will be collected, and how the tool uses, stores, and shares PII with third parties prior to using any government-held PII in an AI system;

(C) Must train employees about the risk of inputting sensitive or PII into publicly available AI systems that use inputs to train the model and share those inputs with other users of the AI system outside of the governmental entity; and

(D) Must strive to practice data minimization and ensure they abide by any purpose limitations granted when the PII was first collected, or as expressly allowed by law.

(i) Security

(1) AI systems are subject to security vulnerabilities. Common security concerns in the AI context may include data poisoning or malicious code injection, exfiltration of models or data within the AI system, and improper access controls that result in unauthorized access to the AI system itself. Secure AI systems will maintain the confidentiality and integrity of the AI system as well as the data it contains even when unexpected events or changes in their environment or use occur.

(2) Governmental entities:

(A) Must monitor, secure, and test AI systems to prevent or limit security attacks; and

(B) Must demand that AI system providers disclose known vulnerabilities and resolutions in a timely manner to the governmental entities deploying those systems.

(j) Accountability and Liability

(1) While governmental entities may delegate tasks and decision making to AI systems, the entities remain accountable for the decisions the AI systems make and the outcomes they produce. Use of AI systems for employment-related tasks or to make consequential decisions poses heightened risks.

(2) Governmental entities:

(A) Must provide training to employees on how to use AI systems in an effective, safe, and ethical way;

(B) Must ensure their vendors are contractually bound to these AI ethical principles and any relevant laws or regulations governing the use of AI systems; and

(C) Must ensure AI systems they deploy comply with the legal obligations they have at both the state and federal level.

(3) When deploying AI systems, governmental entities must establish appropriate retention schedules for the AI system's records and consider the Public Information Act implications related to the storage of data inputs and outputs.

(k) Evaluation

(1) AI systems can change over time, as can the purposes for which they are used.

(2) Governmental entities:

(A) Must establish methods for regular evaluation of AI systems to ensure the systems provide ongoing benefit to the populations they serve; and

(B) Must document such evaluations.

(l) Documentation

(1) Documentation provides a critical element for managing AI risk. Consistent documentation of preliminary assessments, ongoing monitoring and testing, and complaints provides governmental entities insight into the operations and improvements of their AI systems over their lifecycle. Documentation allows entities to evaluate the value of AI systems and determine where best to spend resources in further developing AI solutions.

(2) Governmental entities should maintain records of:

(A) The sources of data used in the AI system; and

(B) How the AI system is modified throughout the system's life cycle.