

**DRAFT Neutral Guidelines: Use of Artificial Intelligence**

**Purpose**

* Artificial Intelligence (AI) can greatly benefit organizations by analyzing data, transforming processes and improving decision-making skills. AI also has ethical and legal implications, particularly in areas such as bias, privacy and the potential for misuse when generating content.
* JAMS provides these guidelines to promote the adoption of AI, aiding neutrals in navigating its complexities and potential risks. Our aim is to ensure the responsible and effective utilization of AI across the organization.
* Moreover, AI regulation is constantly evolving at the state, national and international levels. While these guidelines are intended to assist in compliance with such regulations, they do not encompass all measures necessary for full legal and ethical compliance.
* Since AI continues to change rapidly, JAMS is committed to updating these guidelines to support you and provide relevant guidance.

**Context**

To help shape these guidelines, it is important to understand some fundamental aspects of AI:

* What is **AI**? There is no one definition of AI. The term “artificial intelligence” generally means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Put simply, humans train systems to make sense of data. How “smart” these systems are is dependent upon many factors—a lot like humans.
* **Input data** is data added to an AI platform to explain a problem, situation or request. Input data may be cleaned, labeled and organized, or it may be raw data. Often an AI is asked to create or synthesize information based on input data and the AI’s algorithm to create new data, or **output data.** AI can also be used to make decisions (**decision-making**) if it is tasked with deciding the outcome of a question**.**
* What is an AI **hallucination**? A hallucination is a nonsensical or erroneous output. Humans train these systems, so there can be errors.
* **Open AI systems**, such as OpenAI's ChatGPT, are characterized by their vast databases and the ability to learn from a wide array of public contributions continuously. These models are accessible to developers, researchers and businesses, allowing for a broad range of applications, from generating creative content to assisting with coding. The open nature of these systems offers unparalleled flexibility and innovation potential, inviting users to explore the limits of machine learning and natural language processing.
* However, this openness comes with inherent risks. The lack of control over data sources can lead to potential biases, inaccuracies and even security vulnerabilities. Open systems often operate in a regulatory gray area, raising concerns about privacy, misuse and ethical implications. The need for robust governance and ethical frameworks becomes more pressing to ensure responsible use and to safeguard against malicious exploitation.
* In contrast, **closed AI systems** are defined by their controlled environments. They operate within specific parameters, using preselected and vetted data sources to ensure accuracy, reliability and security. However, given the constraints, they lack the robustness of an open AI system.

**Guidelines**

* JAMS presents these guidelines to facilitate the adoption of AI technology among Neutrals, enabling you to navigate the complexities of AI and its potential risks. We aim to foster responsible and effective utilization of AI across the organization, promoting informed decision-making and ethical practices.
1. **Confidentiality**
	* Some AI models, called large language models, or LLMs, are designed to process and generate language based on the input received. While these generative AI models can serve as tools that provide helpful insights and responses, they can log each user query. *Some* systems are not inherently equipped to properly deal with personal information, or PI (defined below); sensitive personal information, or SPI (defined below); or confidential information, or CI (defined below). Examples of LLMs include OpenAI – GPT, Meta – LLaMA, Google – PaLM/Bard, Claude, LaMDA, BLOOM, Bert and Falco.
	* If a Neutral includes CI in their AI queries and conversations in open systems, that information can resurface in responses to other users worldwide and violate their confidentiality obligations.
	* Additionally, such models are generally not bound by the same confidentiality agreements.
	* Neutrals should understand the confidentiality obligations in their jurisdiction and use only AI tools that can guarantee the safeguarding of CI according to the relevant requirements.
2. **Privacy**
	* The introduction of PI or SPI, subject to the California Consumer Privacy Act, as amended (CCPA) and other applicable privacy laws, into AI models where we lack the appropriate permission and contractual obligations may violate privacy regulations. Introducing this information into such models may lead to monetary penalties, reputational damage and litigation. This is intended to include all PI and SPI collected at JAMS in accordance with the JAMS Privacy Policy.
	* Neutrals should anonymize (defined below) any PI and SPI if using open AI systems or other AI tools that have not been carefully vetted to understand the technology and its security.
	* It is important to note that JAMS does not sell PI/SPI.
3. **Duties**
	* Parties agree to use JAMS and our Neutrals to obtain services. JAMS and the Neutrals are contractually and ethically obligated to provide those services and not delegate or abdicate them.
	* Neutrals may use AI to supplement their services, but they cannot substitute their work with AI. Accordingly, Neutrals must refrain from overreliance on AI, and inputs and outputs should be carefully analyzed for accuracy, bias and hallucinations.
	* Furthermore, Neutrals must exercise caution against excessive dependence on AI systems. Rigorous scrutiny of both inputs and outputs is essential to ensure accuracy while diligently identifying and addressing any potential biases or misleading interpretations. Such meticulous analysis guards against erroneous conclusions or hallucinations within AI-driven processes.
	* Neutrals must uphold their obligations, including adherence to the JAMS Mediator Ethics Guidelines and JAMS Arbitrator Ethics Guidelines.
	* If neutrals adhere to these guidelines, disclosure of AI usage is not mandatory unless deemed necessary by the Neutral due to specific circumstances, notwithstanding legal requirements. In such cases, prompt communication to all parties involved is essential.
4. **Intellectual Property**
	* There is an inherent risk that the output of the AI platform is not copyrightable. It is important to thoroughly review and understand who has the right to use the property (for the input) and who will own the property of the output in order to mitigate intellectual property issues.
	* AI use is not permitted when the intellectual property, copyright and/or ownership of an AI-produced product, such as JAMS Access or other JAMS systems code, may be questioned.

**Points of Contact**

* JAMS is committed to maintaining an open dialogue about this ever-evolving field. We eagerly anticipate the opportunity to enhance the JAMS experience for our clients, associates and panelists through responsible AI usage.
* Should you have questions about AI or these guidelines, please contact the following JAMS associates in addition to your business manager:

**Nate Brooks:** **nbrooks@jamsadr.com**

EVP, CFO & COO

**William Zauner:** wzauner@jamsadr.com

Senior Vice President, Chief Information Officer

**Alicia Jantsch, Esq., CIPP/US:** ajantsch@jamsadr.com

Senior Counsel, Privacy & Compliance

**Guideline Definitions**

* **Personal information (PI):** Any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual. Examples include, but are not limited to, personal unique identifiers such as full name and federal or state-issued identification numbers; personal information such as telephone number, address and financial information; characteristics of protected classes under state or federal law; internet or other electronic network activity information; audio and visual information; employment information such as work history and prior employers, information from background checks and resumes; education information such as student records and confirmation of graduation; and inferences based on information about an individual to create a summary about, for example, that individual’s preferences and characteristics. PI does not include publicly available information that cannot be attributed to an individual because, for example, it has been aggregated with other information (e.g., statistical information) or otherwise anonymized in such a way that one cannot reasonably attribute it to a specific individual.
* **Sensitive personal information (SPI):** A subset of PI that carries more risk if it is exposed than PI. Examples include, but are not limited to, an individual’s physical or mental health/condition; genetic and biometric data; precise location; race/ethnicity; religious or philosophical beliefs; union membership; sexual activity or orientation; Social Security, driver’s license, state identification card or passport number; contents of mail and email and text messages unless the JAMS is the intended recipient of the communication; and account login, financial account or debit or credit card number in combination with any required security or access code, password or credentials allowing access to an account
* **Confidential Information (CI):** Information acquired while providing ADR services at JAMS regarding clients, attorneys who represent said clients, employees of JAMS and independent contractors of JAMS that is considered confidential and that has been subject to reasonable measures to protect its confidentiality or is required by law to be protected as confidential information. CI includes, but is not limited to, case, party and attorney information (including contact information for such party and attorney); JAMS financial information; neutral revenue information; JAMS software and computer programs; JAMS system of operations and procedures, including methods of marketing services, setting cases, special programs and fee policies; information created or provided by the JAMS Institute; and JAMS business plans and strategies.
* **Neutral:** An individual classified by JAMS as providing ADR services in association with JAMS.
* **Anonymized:** Data that cannot reasonably identify, relate to, describe, be associated with or be linked, directly or indirectly, to a particular consumer.