Administrative Policy No. 15.28

Subject:	Use of Artificial Intelligence
Information Contact:	DSHS Chief Enterprise Architect (360) 902-7516
Authorizing Source:	Executive Order 24-01 Artificial Intelligence
Effective Date:	April 15, 2025
Revised:	NEW
Approved By:	**Original approved by Pearlette J. Ramos** Senior Director, Office of Justice and Civil Rights

Purpose

The purpose of this policy is to ensure legal, ethical, equitable, and secure use of any artificial intelligence (AI) technology including, but not limited to, generative AI. It defines acceptable and prohibited uses and outlines the Department of Social and Health Services (DSHS) obligations related to the use or development of AI models and systems.

Background

AI is an emerging technology that is increasingly more powerful. AI development must incorporate safe and ethical use while meeting all current RCWs, WaTech policies and standards, DSHS policies, DSHS information security and technology standards, and legal regulations.

Scope

This policy applies to all DSHS organizational units, staff, interns, and volunteers for the use of any AI applications or development of AI models, including internal models, third-party models, and publicly available applications.

Additional Guidance

- RCW 39.26 Procurement of goods and services
- RCW 39.34 Interlocal cooperation
- RCW 43.19 Department of enterprise services
- WaTech artificial intelligence resources
- DSHS administrative policies
    - DSHS AP 5.01 Privacy policy – safeguarding confidential information
    - DSHS AP 5.02 Public records requests
    - DSHS AP 13.08 Operational (purchased) goods and services
    - DSHS AP 13.10 Central contracts and legal services (CCLS)
    - DSHS AP 13.12 Competitive solicitations
    - DSHS AP 13.25 Vendor agreements and non-standard contracts
    - DSHS AP 15.10 Information security
    - DSHS AP 15.21 Information technology standards compliance
    - DSHS AP 15.25 DSHS information technology governance
    - DSHS AP 18.64 Standards of ethical conduct
    - DSHS AP 18.91 Use of resources

Definitions

Artificial intelligence (AI) – Any software, system, or application that uses machine learning, natural language processing, neural networks, or any other technology designed to simulate human intelligence. AI enables computers and devices to perform tasks that usually require human intelligence. It is capable of self-learning, understanding language, recognizing patterns, and making decisions. AI helps solve complex problems and automate tasks.

AI-generated data – Data produced by an AI system or service. This includes any responses or output from queries, research, analysis, requests, etc., submitted to an AI system. AI-generated data results from integrating input data with processing and data resources internal to the AI system.

Automation bias – Over-relying on the outputs of AI systems without considering other sources of information. Simple example: typing a word correctly in a Word document, but accepting an auto-correction, because you think the Word application must be right.

Data integrity –The assurance that data remains accurate, consistent, and reliable throughout its entire lifecycle and is not altered without authorization.

Generative artificial intelligence (Gen AI) – A type of AI that uses machine learning models, such as neural networks, to generate new content, including text, images, audio, video, or code. These models are trained on large datasets to learn patterns and can create original outputs that mimic human-like creativity. Common examples include language models like ChatGPT, image generators, and code generation tools. Generative AI poses specific risks, including the potential for data leaks, misinformation, and ethical concerns, especially when handling confidential or sensitive information.

High-risk generative AI system – System using generative AI technology that creates a high risk to natural persons' health and safety or fundamental rights. Examples include the use of biometric identification, critical infrastructure, employment, health care, law enforcement, and administration of democratic processes.

Machine learning – The basic concept of machine learning in data science involves using statistical learning and optimization methods that let computers analyze datasets and identify patterns. Machine learning techniques leverage data mining to identify historic trends and inform future models. (UC Berkeley School of Information, 2020)

Policy Requirements

Artificial intelligence is a powerful technology that has the potential to greatly benefit the DSHS mission by streamlining DSHS business processes and improving service delivery. The use of AI also has the potential to introduce risk for DSHS and our clients if not properly managed.

1. Use of Artificial Intelligence
    a. All uses of AI, including generative AI must:
        i. Be reviewed and approved prior to use;
        ii. Meet all privacy, retention, copyright, security, confidentiality, and any other regulatory requirements; and
        iii. Follow all established IT governance procedures.
    b. Any updates that add new AI functionality or capability to existing approved software or services must go through the DSHS intake review and approval process before use.
    c. Use of AI is limited to DSHS business purposes. [See DSHS AP 18.91 Use of Resources]

2. Procedures to procure or develop an AI system
    a. Develop a business use case that clearly defines the business need.
    b. Submit the business use case to the DSHS intake to begin the process. This is the same process required for all IT investments.
    c. All AI systems must be listed in the DSHS IT portfolio. The DSHS IT portfolio team adds the information to the DSHS IT portfolio when a system is assessed as part of the DSHS intake process.
        i. In addition, all generative AI systems and high-risk generative AI systems must be specifically identified as such in the DSHS IT Portfolio.

3. Contracting requirements
    a. Any and all acquisitions of AI products, development of AI solutions, AI systems, AI applications, AI services, AI software, including, but not limited to, robotic processing, bots and chatbots, must comply with the following DSHS administrative

policies. All acquisitions must be acquired using an allowable and approved DSHS contract, interagency agreement, outside vendor agreement, DSHS purchase order, or software licensing agreement; to include a DSHS contracting signatory review, negotiation, and approval (to include click-through agreements).

i. DSHS AP 13.08 Operational (purchased) goods and services;
ii. DSHS AP 13.10 Central contracts and legal services (CCLS);
iii. DSHS AP 13.12 Competitive solicitations; and
iv. DSHS AP 13.25 Vendor agreements and non-standard contracts

b. A data-share agreement must be in place before sharing any DSHS data with a third party.

4. Mitigating the risk to DSHS while benefiting from the use of AI technologies

a. Need for human review:

i. All AI-generated content requires human review and validation prior to use or distribution, especially when used in official DSHS capacities.

1. Final agency decisions, especially those that impact an individual's benefits, rights, or freedoms, must always involve human review and validation.
2. Some AI-generated content can be inaccurate, misleading, or fabricated, which is why all AI-generated content requires review and validation prior to use or distribution.

ii. AI-generated content reviews must evaluate and verify:

1. The content is accurate, relevant, and free of potential biases to facilitate ethical use;
2. No copyrighted material is published without appropriate attribution or the acquisition of necessary rights; and
3. AI-generated content used in official state capacity is clearly labeled as such, and details of its review and editing process (how the material was reviewed, edited, and by whom) are available.

5. Roles and responsibilities

a. Administrations are responsible for:

i. Developing procedures for reviewing AI-generated data and information for AI systems they administer.
ii. Developing and maintaining documentation that describes the "how" and "why" behind actions, decisions, and processes that use AI-generated data and information.
iii. Develop procedures to inform individuals if a decision or outcome affecting them is determined with the use of AI-generated data or information and how to submit a request for review.
iv. Ensuring employees receive sufficient AI training consistent with:

1. Individual roles and responsibilities; and
2. Applicable AI system-specific requirements, including;

        a. The scale, complexity, risk level, and sensitivity of the AI system; and
        b. Recognizing and addressing automation bias in AI-generated content.
    b. Employees are responsible for the review and validation of any content they produce or publish, regardless of the method used to create the content, which includes AI-generated material.

6. Privacy and Data Protection
    a. All AI technologies used by DSHS must follow privacy and data protections, and maintain data integrity as identified in federal and state laws, WaTech policies and standards, and DSHS policies and standards.
    b. Personally identifiable information (PII) and personal health information (PHI) of DSHS clients and employees are subject to legal restrictions and are considered Category 3 or Category 4 data. Any use of an AI platform that involves PII or PHI requires a written agreement that:
        i. Must include a business associate agreement for PII or PHI of a HIPAA-covered health care component;
        ii. Restricts the use of the data to the purpose of the agreement; and
        iii. Prohibits redisclosure of the data without DSHS approval.
    c. All publicly available AI systems must be assumed to be insecure until they have been through DSHS intake, including the security design review process, and are approved for use.
        i. Unapproved systems create the risk of unauthorized disclosures of sensitive or confidential data, legal liabilities, and other consequences.
    d. All internally-developed AI systems must go through DSHS intake, including the security design review process, and be approved before use.

7. Transparent, auditable, explainable, and interpretable
    a. DSHS employees must be able to interpret and explain any actions taken by, or as a result of, the AI system to ensure fair, accurate, and unbiased outputs.
    b. Documentation must be created, maintained, and available to describe the “how” and “why” behind actions, decisions, and processes.

8. Violation of Policy
    a. A DSHS employee, intern, or volunteer violating this policy may be subject to disciplinary action up to and including dismissal.