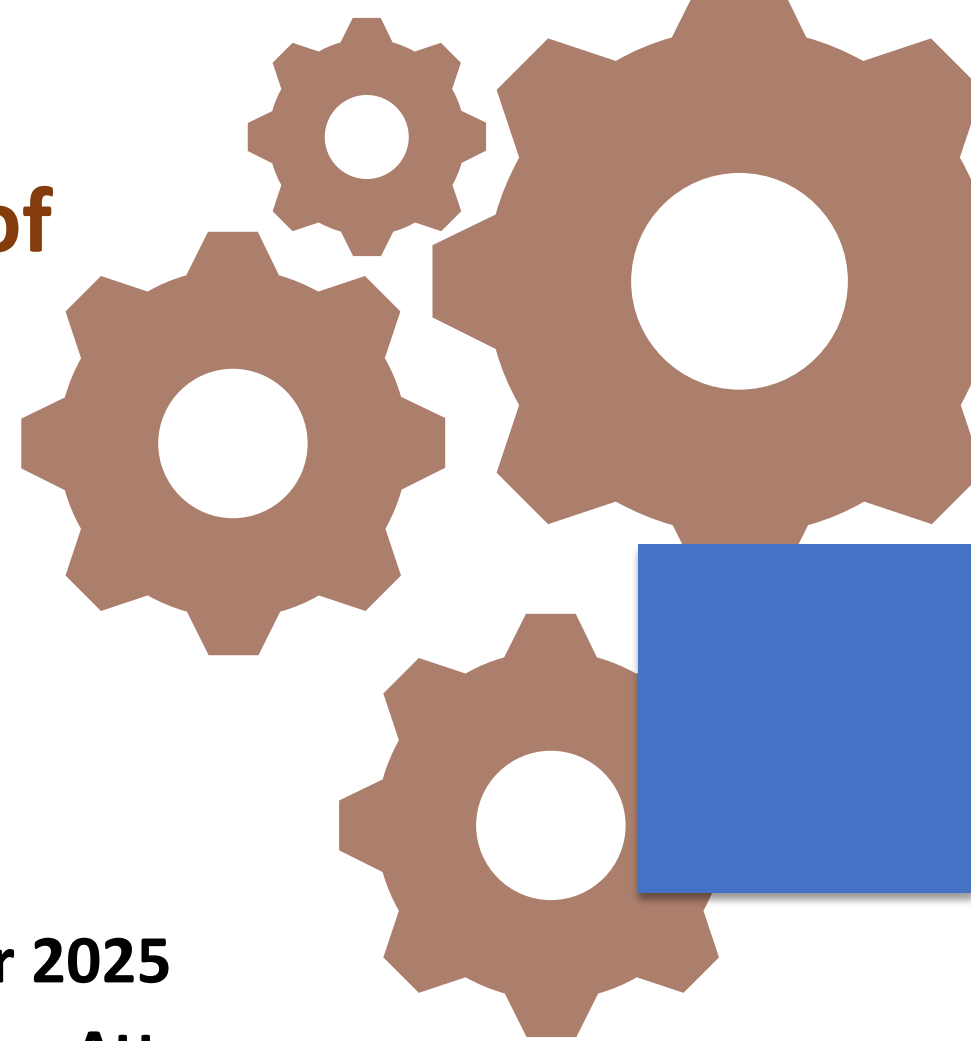# The Legal Rewards & Risks in the Use of Artificial Intelligence in Social Services Operations
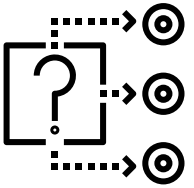
NYPWA Conference: Winter 2025

Paula Mallory Engel, Chief Welfare Attorney

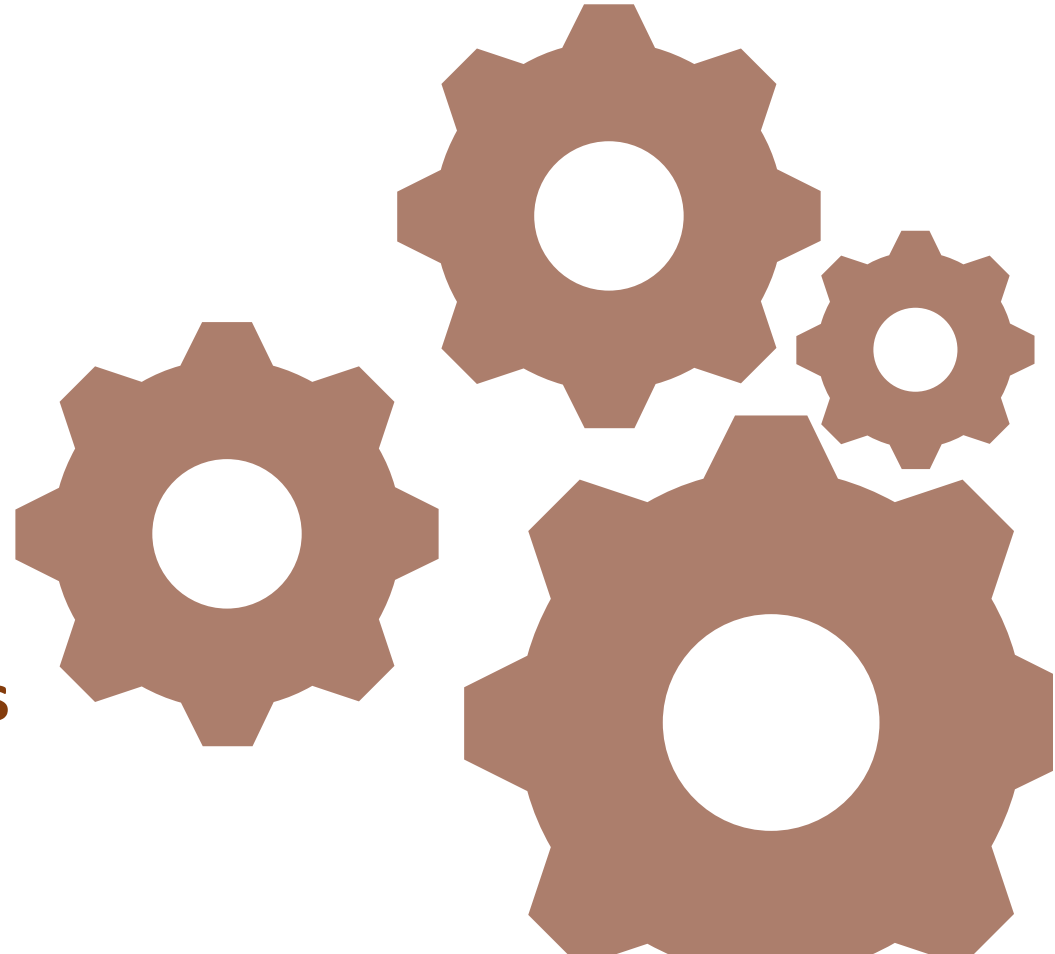**Onondaga County**

Purpose

To help LDSS Attorneys and Management understand the AI concept, how it can benefit operations, and how to assess and minimize its risks.

Overview

- **Learn what real AI is**

- **Understand legal landscape (Federal and State)**

- **Be aware of risks and benefits of potential use**

- **Learn some best practices for managing risks**

What is "Artificial Intelligence," Really?

- **Phrase "AI" coined in 1955 by Stanford U. professor**

- **AI combines computer science and datasets to simulate human intelligence and enable problem-solving, using "machine learning"**

- **Machine learning is the process of using historical data to predict and share new output**
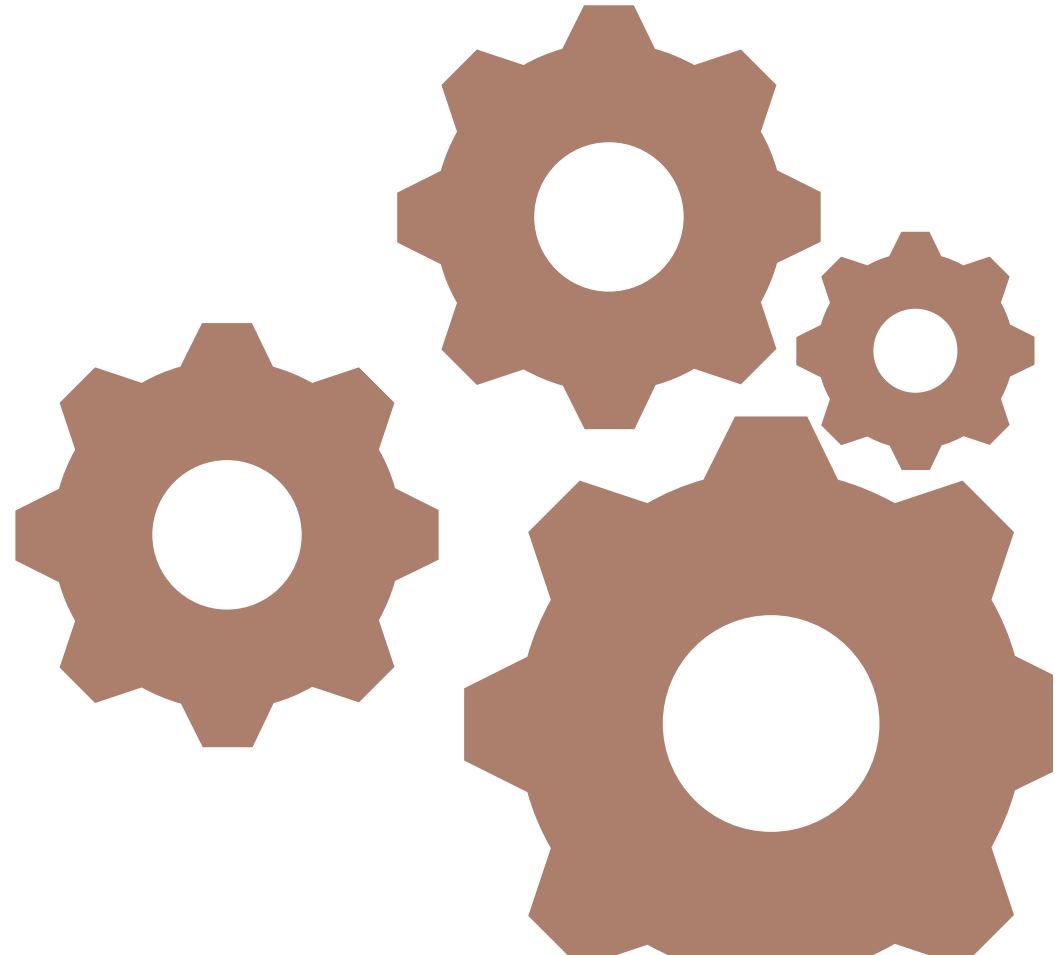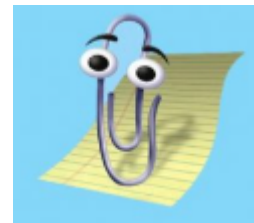
Older ChatBots are not always true "AI"

AI virtual assistants:

➤ Handle more advanced applications

➤ Leverage natural language processing and machine learning ("ML") capabilities

Clippy-type Digital assistants:

➤ Run on simple (Bayesian) algorithms

➤ Rely on rules and templates (not "ML")

Define "Artificial Intelligence" and "Machine Learning"

The term machine learning (ML) is often used interchangeably with the term artificial intelligence (AI), but ML is a subfield of AI.

Artificial intelligence (AI) - the ability of a system to handle representations, both explicit and implicit, and to perform tasks that would be considered intelligent if performed by a human.

Machine Learning (ML) – processing data, learning from experience and improve systems/task

Deep learning - a type of an ML algorithm designed to mimic a human brain's neural network

Generative AI (also known as GenAI) – another type of ML algorithms, which can create content, including text, imagery, video, simulations, code, audio and more.

Examples of generative AI include tools such as ChatGPT, DALL-E and Google Bard.

COMPUTER SCIENCE

ARTIFICIAL INTELLIGENCE

MACHINE LEARNING

-Deep Learning
-GenAI
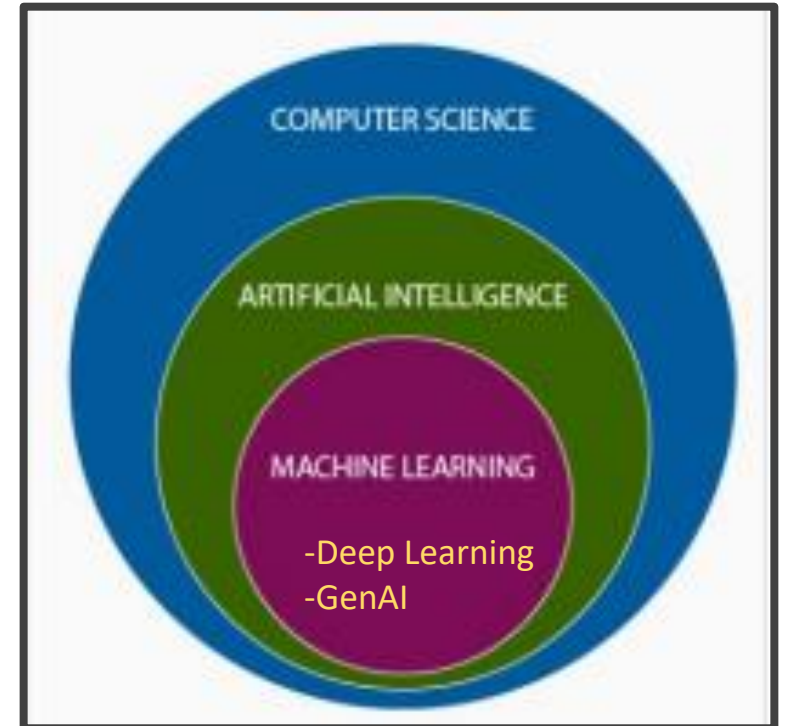
How do Business Owners use AI? How might the LDSS?

Top Ways Business Owners Use Artificial Intelligence

Forbes Advisor surveyed business owners to find out how they currently use or plan to use AI within their business

Potential LDSS Uses

Use	Percentage	LDSS Use
Customer service	56%	Call Centers
Cybersecurity / Fraud management	51%	Recipients/Contractors
Digital personal assistants	47%	
Customer relationship management	46%	
Inventory management	40%	Housing, Child Care
Content production	35%	
Product recommendations	33%	
Accounting	30%	
Supply chain operations	30%	Staffing Models, Contract Needs
Recruitment and talent sourcing	26%	Sorting through Resumes for Qualifications
Audience segmentation	24%	

Source: Forbes Advisor • Embed

Forbes ADVISOR

FEDERAL LAW: AI Executive Order 14110 of 2023

The <u>Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence</u> (EO), signed by President Biden on October 30, 2023, provides some direction regarding US policy. It establishes a framework for managing AI risks, directs federal action to regulate the use of health AI systems, and guides the development of tools to advance AI innovation across sectors, including health.

FEDERAL LAW: AI Executive Order 14110 of 2023 Background

1) Far Information Practice Principles (FIPPs), 1973 Advisory Committee to US Department of Health, Education and Welfare: "*Records, Computers and The Rights of Citizens*"

2) EO 13960 – "*Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*" (Biden, October 2023)

3) ~~EO 13985 – "*Advancing Racial Equity and Support for Underserved Communities Through the Federal Government*" (Biden, Jan. 2021)~~ **Rescinded by President Trump 1/20/2025**

AI Executive Order 14110 of 2023

Eight guiding principles and priorities – the first six apply to the LDSS:

(1) ensure safe and secure AI technology;

(2) promote responsible innovation, competition, and collaboration;

(3) support American workers;

(4) advance equity and civil rights;

(5) protect American consumers, patients, passengers, and students;

(6) protect privacy and civil liberties;

(7) manage the federal government's use of AI; and

(8) strengthen US leadership abroad, promoting safeguards so that AI technology is developed and deployed responsibly
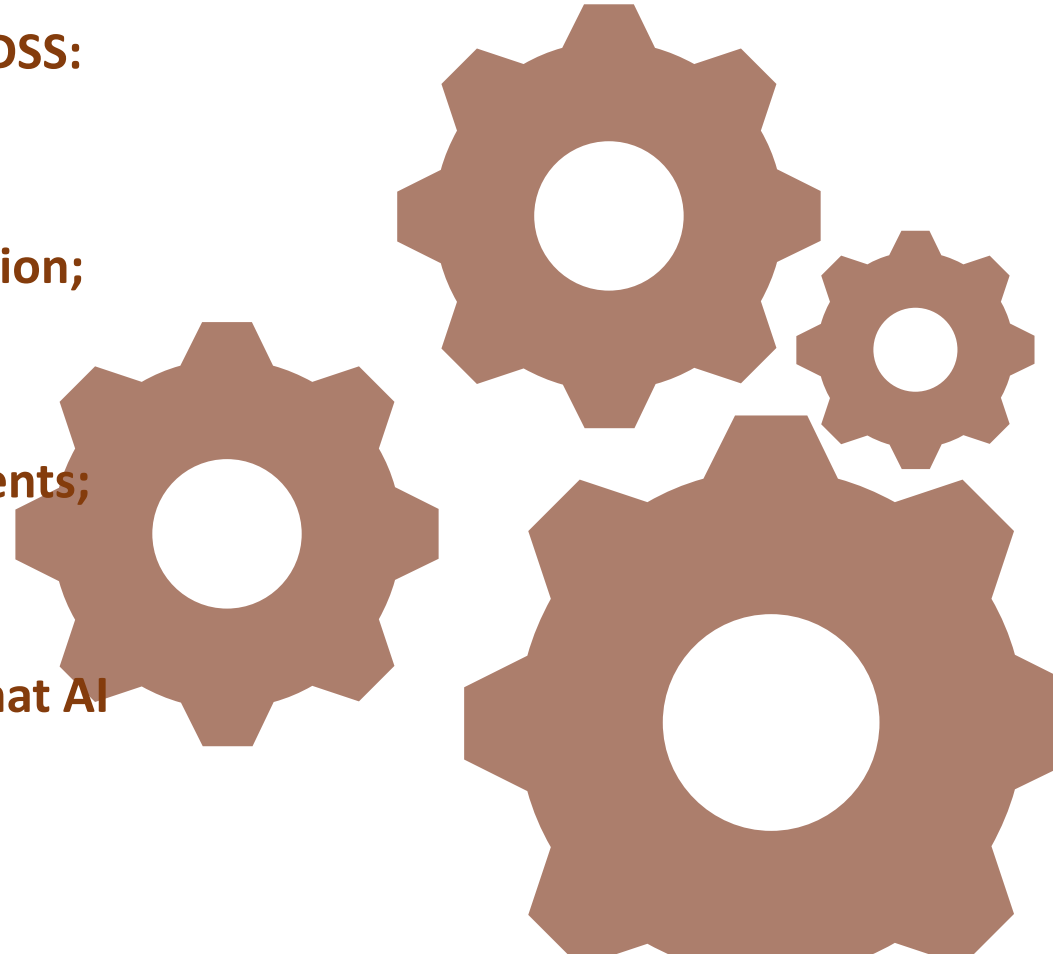
AI Executive Order of 2023 – Risks Remain

- **Exacerbating service/access disparities**

- **Compromising the privacy of intimate personal information, and**

- **Triggering improper decisions that could be harmful**
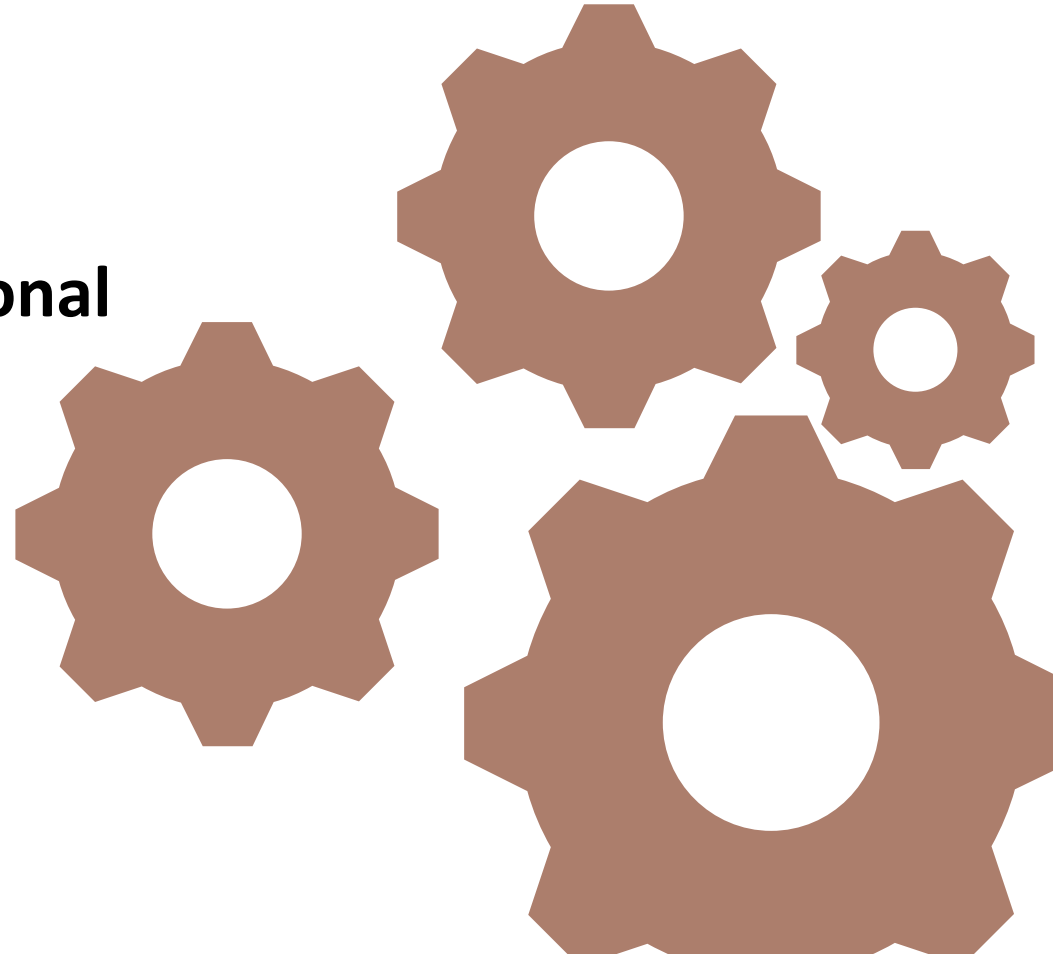
Framework for Safe Deployment of AI – Released by US Homeland Security Nov. 2024

Public Sector Roles and Responsibilities

Cloud and Compute Infrastructure Providers

AI Developers

Critical Infrastructure Owners and Operators

1. Deliver essential services and emergency response
2. Drive global AI norms
3. Responsibly leverage AI to improve the functioning of critical infrastructure
4. Advance standards of practice through law and regulation
5. Engage community leaders
6. Enable foundational research into AI safety and security
7. Support critical infrastructure's safe and secure adoption of AI
8. Develop oversight

Question: How does HHS use AI?

HHS/ACF released its opportunities, challenges, and risk assessment report on AI in September, 2022:

Tasked in 2020 to do a study with three objectives:

(1) Understand AI and how HHS could leverage it

(2) Understand existing and potential **barriers, facilitators, risks and benefits**

(3) Identify options and opportunities to address and mitigate the existing and potential risks, as well as promote benefits of using AI in mission work.

The 9/22 report addresses Objective #3: Risks and Benefits

Question: How does HHS use AI?

HHS developed its AI Strategic Plan in late 2024, released it on 1/15/2025

- Examples of Uses: Children Welfare Information Gateway - a hotline for answering questions or requesting information on resources: https://www.childwelfare.gov/stay-connected/contact/ (implemented 6/2020)

- Collective Bargaining Questions and Answers (output is screened by Large Language Models or "LLMs")

Question: How does HHS use AI?

9/22 report - <mark>Benefits and Challenges of AI Identified</mark>:

Benefits:

1. **Improving mission-oriented processes and services** (service delivery improvements, task automation, cost savings, resource use efficiencies

2. Enabling **larger scale analyses** (greater insights possible by drawing on diverse data sets across systems)

3. Potentially increasing **personalization and targeting** (improve placement recommendations or improve matching users to services)

Question: How does HHS use AI?

9/22 report - Benefits and Challenges of AI Identified:

Challenges, Part I:

1. **User confidence and trust** (justified trust [tested abilities/usefulness/accuracy of output) versus public trust

2. **Model performance** (testing abilities/usefulness/accuracy of output – justified trust)

3. **Maintaining privacy** (Greater privacy protections may decrease utility but increase public trust)

Question: How does HHS use AI?

9/22 report - <mark>Benefits and Challenges of AI Identified</mark>:

Challenges, Part II:

4. **Bias** (can come from skewed data sets, systemic bias in data capture/use, human bias in development and output interpretation)

5. **Data and dataset quality** ("garbage in, garbage out")

6. **Transparency and explainability** (Lack of clarity can result in decreased public trust, decreased ability to test or understand how the outputs are generated)

7. **Capacity** (Do you have the subject matter and IT staff expertise, computing infrastructure to develop, manage implementation, test and evaluate AI outputs?)

HHS Directives to States on AI Use

(1) Perform a risk assessment at each stage of the process:

    (a) Choosing and procuring AI technology;

    (b) Designing and governing AI;

    (c) Deploying AI;

    (d) Managing AI.

(2) Follow the 5 Principles of the Blueprint for the "AI Bill of Rights" in EO 14110

(3) When published, follow the national guidelines for security:

    (a) Protect AI models and health data from adversarial attacks;

    (b) Implement data-sharing protocols

    (c) Set a governance model that tests for and reduces misuse from predictive analytics.

HHS Issues Strategic Plans and Toolkits

(1) HHS Plan on AI and Public Benefits (January 2, 2025) – handout

(2) Strategic Plan for the Use of Artificial Intelligence in Health, Human Services, and Public Health (January 2025) – Handout

(3) SNAP – Use of Advanced Automation in SNAP, Memo to SNAP State Agencies (January 10, 2025)

(4) ACF's Strategic Plan for the use of AI (2022) (firewalled)

County Governments are reaching for AI
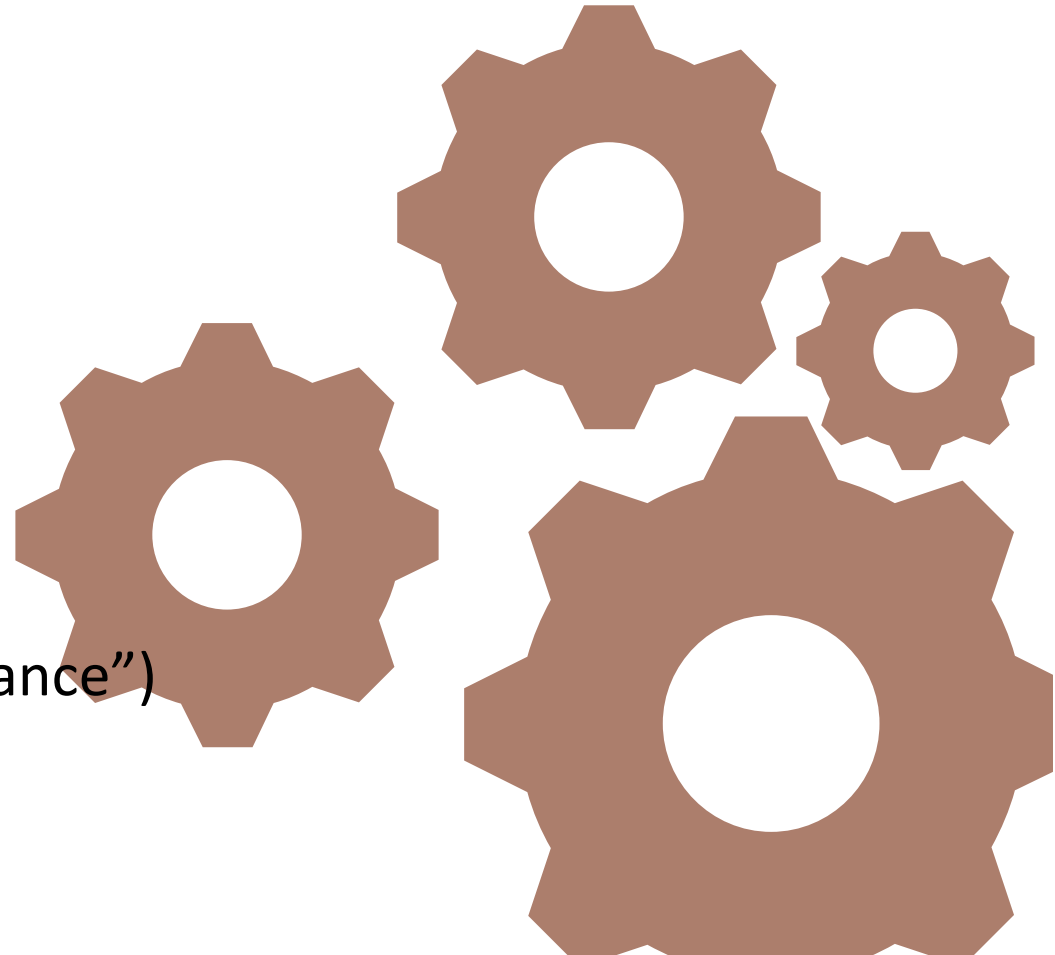
GOALS:
- Reduce manual processes
- Reduce data silos
- ➢ IMPROVED ANALYSIS, PLANNING & EXECUTION

BARRIERS:
- Rigid procurement/compliance rules
- Legacy systems and outdate workflows
- Data complexity across systems
- Need for data security and integrity (data "governance")

Potential Use: *Predictive Analytics* for Scaling Operations to Meet Community Needs

Enhanced Predictive Capabilities

- AI can process vast amounts of data from multiple sources, AI algorithms can **_predict changes in community needs_** with greater accuracy and speed (weather, economic downturns, disasters, seasonal cycles, mass casualty, migrations)

- AI can help agencies to and **_implement effective preparedness strategies_** (staffing, contracting, emergency housing, preventive services, for example), potentially saving lives and reducing economic impacts.

Improved Response Coordination

- **_Coordination among human services agencies_** is crucial. AI can streamline communication and resource allocation, ensuring that the right resources are dispatched to the right places at the right time. This dynamic response capability minimizes response times and enhances the overall effectiveness of human service operations.

Potential Use: Active AI Data Mining for FRAUD DETECTION

■ GenAI Application   ■ AI Application

Workflow Steps With AI/GenAI Applications

Capture Data	Initial Assessment and Triage	Investigate Activity	Mitigate Risk	Resolution
Flag Potentially Fraudulent Activity	Retrieve Customer Information	Retrieve Transaction Data	Decide On Appropriate Mitigation Actions	Confirm Fraudulent Activity
Collect Relevant Data Points	Verify Further Investigation	Assess Behavior Anomalies	Block Account/ Transaction (If Necessary)	Finalize Case and Document Findings
	Assign Investigators	Interview Customer	Approve Mitigation Plan And Escalate To Management	Update Case Status and Feedback Loop For Model Improvement
		Review Account History And Related Activity	Notify The Customer	

Source: LeewayHertz.com: AI in fraud detection: Use cases, benefits, solution and implementation

Potential Use: Direct User Services

- HHS uses AI for Child Welfare Information Gateway to connect public with appropriate services contacts

- AI can help identify appropriate spoken language to engage qualified interpreters faster

- Select NYS districts are developing SNAP call center response systems using AI

Call centers are at the forefront of general AI adoption: conversational AI, Intelligent Virtual Assistants (IVA), call analytics, more efficient routing and more

Potential Use: Minimizing Security Threats

Benefits:

- automate repetitive tasks (log analysis; vulnerability screening)

- accelerate threat detection and response

- improve the accuracy of IT responses to strengthen the security posture against various security issues and cyberattacks

Risks:

- Data breaches and misuse

- Adversarial manipulation of AI

- Vulnerabilities in the AI infrastructure, overreliance on the AI

- Bias and Discrimination

- Lack of transparency

- Cyber-attacks on the AI source-vendor's systems

NEW STATE LAW: NYS State Technology Law Art. 4

- The LOADing Act – Legislative Oversight of Automated Decision-making in government Act

- Effective December 21, 2025

- Workplace protections expire in July, 2028

NEW STATE LAW: NYS State Technology Law Art. 4

Brand new, "groundbreaking" statutory framework for AI, signed into law by Governor Hochul in December, 2024:

"**New York Artificial Intelligence Bill of Rights**" also known as Legislative Oversight of Automated Decision-making in government act, or the "LOADing Act", eff. 12/21/2024

Enacts the New York artificial intelligence bill of rights to provide residents of the state with rights and protections to ensure that any system making decisions without human intervention impacting their lives do so lawfully, properly, and with meaningful oversight. Adds NYS Tech Law §§ 401-404

NEW STATE LAW: NYS State Technology Law Art. 4

- NY State Tech Law § 402(1) (effective 12/21/2025):

    "No state agency, or any entity acting on behalf of such agency…" can use AI directly or indirectly that

- affects the delivery of a public assistance benefit;

- has a material impact on the rights, civil liberties, safety or welfare of any individual within the state; or

- Affects any statutorily or constitutionally provided right of an individual

[shall] use that AI system unless the system is subject to "continued and operational meaningful human review"

NEW STATE LAW: NYS State Technology Law Art. 4

- NY State Tech Law § 403: IMPACT ASSESSMENTS

      If a state agency (by itself or through the LDSS, based on §402) wants to use AI for social services or other rights-implicated work, there needs to be an initial report, and then a re-assessment report every 2 years after, <mark>signed by the individual(s) "responsible</mark> for meaningful human review for the lawful application and use of such automated decision-making system." NYS Tech Law § 403(1)

NEW STATE LAW: NYS State Technology Law Art. 4

NY State Tech Law § 403(2): IMPACT ASSESSMENTS (eff. 12/21/2024)

Required contents of report:

(a) Description of objectives of the AI system

(b) Evaluation of the ability of AI to achieve those objectives

(c) Description and evaluation of the objectives and development of the automated decision-making system

    i.   Summary of the algorithms, models, tools

    ii.   Design and training data used to develop the AI

NEW STATE LAW: NYS State Technology Law Art. 4

NY State Tech Law § 403(2): IMPACT ASSESSMENTS (cont'd)

Required contents of report:

d) Testing for i. accuracy, fairness, bias, discriminatory results; ii. Cybersecurity and privacy risks and implemented safeguards; iii. Public health or safety risks of using the AI; iv. Foreseeable misuse and safeguards to mitigate that risk

e) Use of private data, control by users of that data, safeguarding of data

f) IF AI results in discriminatory or biased outcomes, the agency must cease use of system or outputs

g) Impact on employment and civil service – must disclose AI-related layoffs – the first legislation of its kind (sunsets in July, 2028).

NEW STATE LAW: NYS State Technology Law Art. 4

NY State Tech Law § 404: DISSEMINATION OF IMPACT ASSESSMENTS (effective 12/21/2024)

(1) Must go to **governor and legislature** at least 30 days prior to the implementation of the AI system;

(2) Must be **published on agency website** unless some or all of it needs to be redacted because of a written, explained, identified risk to health, safety, privacy or agency infrastructure – specifically if the AI is used for security or program integrity purposes;

(3) Existing AI systems (pre-12/21/2025 implementation) must have filed impact assessments by December 21, 2026.

STATE LAW: NYS Information Technology Policy

- **Issued by NYS Office of Information Technology Services (OITS) on Jan. 8, 2024**

- **Authority under STL § 103(10), Exec. Order 117 (2002) §2**

- **Adopts its own definition of "AI"**

- **Differentiates chatbots, basic if/then, automated or calculated scenarios**
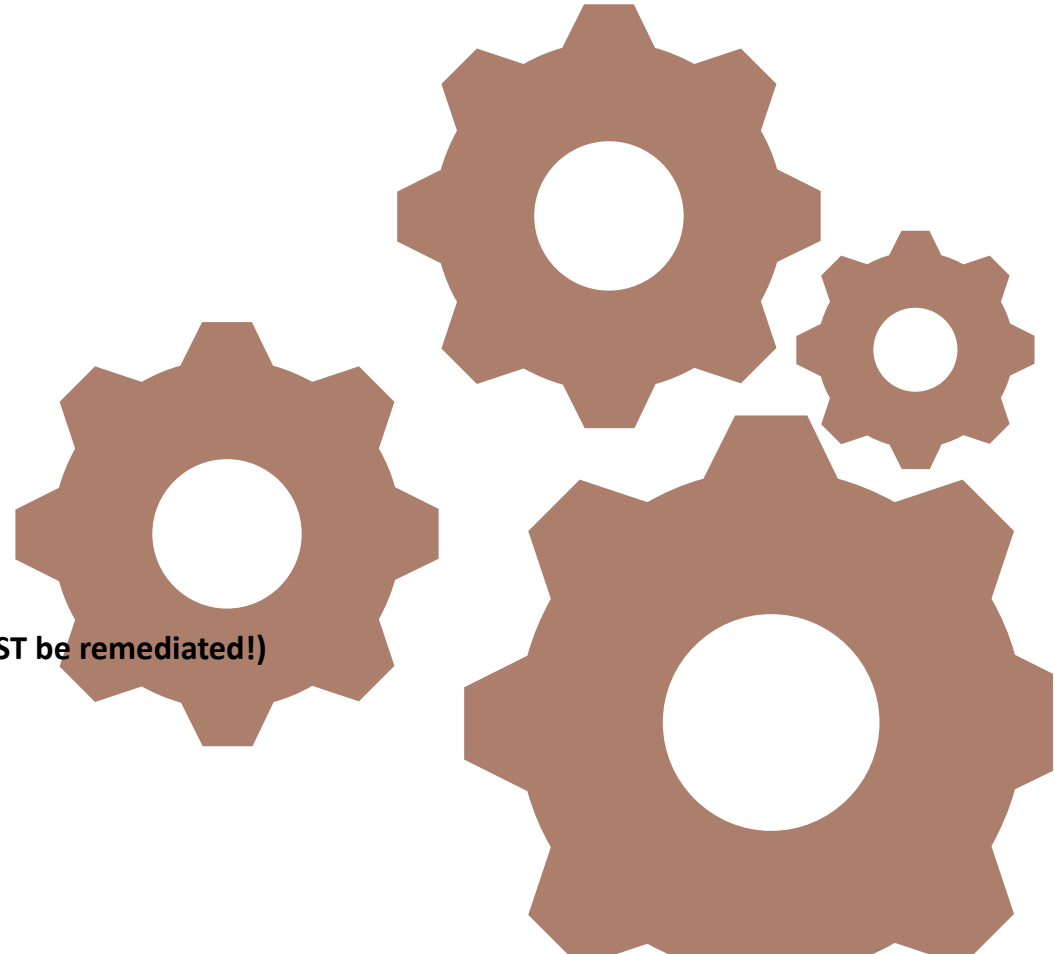
NYS AI POLICY: Required Risk Assessment

- **Security**

- **Privacy**

- **Legal**

- **Reputational**

- **Competency**

- **Any additional risks**
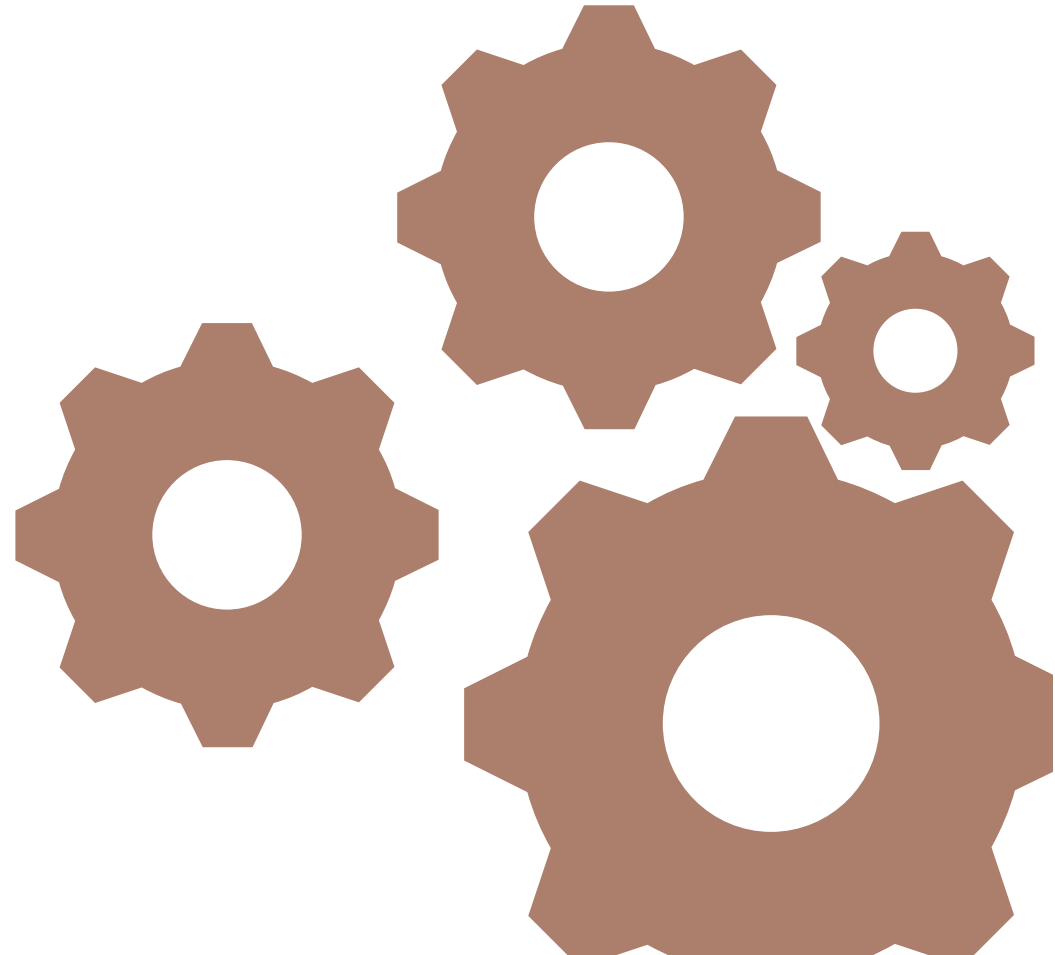
NYS AI POLICY: Requirements

- **Notify State OITS** of use of AI pursuant to OITS guidance within 180 days of issuance of OITS guidance (not yet issued)

- Maintain required **confidentiality**

- Must have **top-level approval** prior to adopting an AI system
-         Sign-Offs from Exec, Law, Operational Mgmt., Ethics Officer

- Identify an **"Information Owner"** for each AI system

- Must have **human oversight, cannot make final decisions**

- Must be **able to explain** how the AI works, is being used

- Continuously **assess (documented) the RELIABILITY, SAFETY and FAIRNESS** of AI output (bias MUST be remediated!)

- **Disclose to Public** how AI is being used, if interacting directly with the AI system

NYS AI POLICY: Required Risk Assessment is Critical to Effective AI Governance

NAM AI/ML Implementation Life Cycle

NYS AI POLICY: Required Risk Assessment SECURITY and PRIVACY

SECURITY:

"Trustworthy AI" is defined as having the characteristics that it is "valid, reliable, safe, secure, resilient, accountable, transparent, explainable, interpretable, privacy-enhanced, and fair with human bias managed." NIST AI RMF

Follow all ITS standards https://its.ny.gov/policies

Complete Privacy Risk Assessment – NIST has a list of tools

NYS AI POLICY: Required Risk Assessment SECURITY and PRIVACY

- ✓ Assess privacy impact

- ✓ Use minimum PI necessary

- ✓ Follow state requirements on retention

- ✓ Ensure accuracy of data inputs and outputs

- ✓ Provide for compliant data disposal

- ✓ Give "data subjects" control and transparency with data processing

NYS AI POLICY: Required Risk Assessment LEGAL and REPUTATIONAL

- Must submit engineering consultation request to OITS and follow NYS-P08-001: Plan to Procure

- Data outputs cannot be biased (Civil Rights Act, Rehab. Acts of 1973 and 1974, ADA, EO 13117 on LEP)

- Data outputs must be accurate, private and secure (aim to prevent actual harm to individuals and families, individuals)

- Intellectual property considerations (using copyrighted elements in an AI inputs and outputs) ex. NY Times v. OpenAI

NYS AI POLICY: Required Risk Assessment LEGAL and REPUTATIONAL (BIAS)

According to IBM:

"AI bias, a/k/a machine learning bias or algorithm bias, refers to the occurrence of biased results due to human biases that skew the original training data or algorithm- if unaddressed, can impact the organization's mission and hinder people's ability to participate in the economy and society."

THINK ABOUT IT:

CHILD WELFARE - SCR reports, removals, foster care placement, TPR
BENEFITS – Studies of disproportionate number of sanctions on black and brown women

Google Researcher Says She Was Fired Over Paper Highlighting Bias in A.I.

Timnit Gebru, one of the few Black women in her field, had voiced exasperation over the company's response to efforts to increase minority hiring.

Share full article   276

Timnit Gebru, a respected researcher at Google, questioned biases built into artificial intelligence systems. Cody O'Loughlin for The New York Times
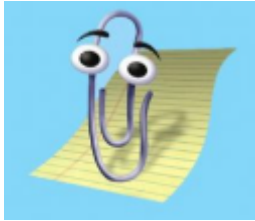
By Cade Metz and Daisuke Wakabayashi

Dec. 3, 2020

NYS AI POLICY: Required Risk Assessment LEGAL and REPUTATIONAL (BIAS)

- "Clippy" - Designed by men as a male agent (he/him pronouns)

- Some women said his gaze created discomfort

HOW DO YOU REDUCE BIAS IN AI?

- Pre-Launch Assessments
  - ✓ Compute performance metrics like accuracy, segmented by gender, race, etc. to reveal imbalances
  - ✓ Proactively calculate bias metrics like disparate impact

- Post-Launch Audits
  - ✓ Dashboard tracking metrics by subgroup
  - ✓ Use "mystery shopper" testing on a human level
  - ✓ Survey impacted groups to assess perception of bias

NYS AI POLICY: Required Risk Assessment COMPETENCY

REPUTATION FOR FAIRNESS, ACCURACY, RESPECT

→

MORE PARTICIPATION AND TRUST IN THE SYSTEM

"Because poor governance leads to poor service delivery, marginalized citizens bear the brunt of the impact of poor governance." *The Impact of Poor Governance on Public Service Delivery: A Case Study of the South African Local Government, International Journal of Social Science and Review. (Apr. 2023, International Journal of Social Science Research and Review, vol. 6, issue 4)*

Best Practices for Implementing AI in your LDSS:

(1) BUILD YOUR ROAD MAP: IDENTIFY OBJECTIVES, PLANNING STRUCTURES AND DECISION-MAKERS

(2) PROVIDE FOR ACTIVE, ON-GOING STAKEHOLDER ENGAGEMENT (INTERNAL & EXTERNAL)

(3) BUILD TRANSPARENCY INTO YOUR STRUCTURES AND SYSTEMS

(4) TEST, TEST and TEST AGAIN, take prompt action on sub-optimal results

Best Practices for Implementing AI in your LDSS:

(1) IDENTIFY OBJECTIVES, PLANNING STRUCTURES AND DECISION-MAKERS

Compliance with state and federal AI law requires a defined development process, a planning and decision-making structure, a data and system governance structure, as well as identifying all responsible decision-makers and roles

Best Practices for Implementing AI in your LDSS:

(2) ENGAGEMENT

- **Identify goals** of Stakeholder Involvement (ShI), and put a process together, including a timeline and feedback to group re: impact

- **Identify/Recruit** members of groups of Sh to be represented – ensure diversity and representation by groups most likely to be adversely affected

- **Report back** to Sh and leadership on what insights were gathered, what changes were made, how Agency will evaluate the impact

Best Practices for Implementing AI in your LDSS:

Engagement | Transparency | Oversight and Feedback

Engagement

- Bring Stakeholders into the planning stage – let them help to identify potential issues and develop strategies to minimize problems

Transparency

- Labels/Warnings

Make sure all applications of AI are appropriately and understandably labeled as AI-generated, and use disclaimers

Oversight and Feedback

- Create an oversight board and detailed policy, training
- Provide a contact for public to provide feedback about accuracy/bias/other issues
- Review and respond to issues, issue report on how issues were resolved

Best Practices for Implementing AI in your LDSS:

(3) TRANSPARENCY (Algorithmic v. Interactive)

- **Algorithmic Transparency** What are the goals, where is the data coming from, how does the algorithm process the data and generate outputs.

- **Conversational Transparency** Let the end-user know how and when they are interacting with AI, and what the AI is going to do with the conversation.

- **Opt-ins and Easy Exits** The more the public has a right to "just say no" to interacting with an AI system, the higher the "public trust" quotient goes

Best Practices for Implementing AI in your LDSS:

(3) TRANSPARENCY (Algorithmic v. Interactive)

- **Algorithmic Transparency**

Most common variables
1.   Name of the system.
2.   System's objectives, tasks, and outputs (Description of what the system does and/or how it does it).
3.   Unit in charge of deploying the system (or responsible unit).
4.   Architecture of the system and techniques and methods used to build the system.
5.   Information on the status of the system and its building process (e.g., conceptual prototype, piloting, production, discontinued, completed)?
6.   Data sources.
7.   Whether the system was developed in-house or with external developers.[21]
8.   Contact information of the unit and/or public official in charge of system's deployment.
9.   Whether personal data was used.
10.   Information about the source code.

Best Practices for Implementing AI in your LDSS:

(3) TRANSPARENCY

The Positive Impacts of Being Transparent (Harvard Business Review, June 2022)

(1) It decreases the risk of error and misuse.

(2) It distributes responsibility.

(3) It enables internal and external oversight.

(4) It expresses respect for people

A special OP/ED note for AI in your Legal Representation of the Agency – Most of the advantages of AI is for private law firm work

Marketed "Pros" of AI:

1. Automate routine and time-consuming tasks (esp. document review)
2. Improved accuracy in forecasting case results (mostly for complex litigation or contract analysis)
3. Cost reduction (but -> NYS Tech Law 402[1])
4. More responsive and personalized client services
5. Expanding access to legal services (IVAs)
6. Continuous learning and improvement
7. Strengthening Competitive Advantage (what competition?)

A special OP/ED note for AI in your Legal Representation of the Agency – But ALL the "cons" apply to government lawyers

Identified "Cons" of AI:

1. Potential for Reduced Human Judgment (lacking consideration of a case's ethical, human or broader social impacts)

2. Data Privacy and Confidentiality Concerns

3. High initial costs and complexity ($$$)

4. Impact on employment (but NYS Tech 402[1])

5. Dependence on unreliable outputs

6. Erosion of Client-Attorney Relationship (and think of all the stakeholders we have)

7. Ethical and legal accountability issues

A healthy skepticism about AI in your legal practice is okay...
"I'm here live, Judge...I...uh...I'm not a cat."

Ethical Considerations for Lawyers using AI

Key Takeaways? BENEFITS of LDSS AI

Artificial Intelligence has the potential to:

(1) Increase efficiency and accuracy

(2) Free up staff to tackle more complex/nuanced work (*but not replace*)

(3) Reduce fraud, waste and abuse

(4) Help deploy resources quickly where really needed

Key Takeaways? RISKS of LDSS AI

Artificial Intelligence has the potential to:

(1) Be a tremendous drain on resources while in development

(2) Require implementing new structures, policies and training, reporting

(3) Need to be constantly checked (bias, accuracy)

(4) Make our districts more vulnerable to cyber-attacks and data theft,
     the more we rely on machine learning to do the work

Key Takeaways? Best AI Practices Roadmap

PRIME DIRECTIVE: Focus on the TRUST IN and TRUSTWORTHINESS OF AI SYSTEMS

- **Address concerns regarding <u>bias</u>.**

- **Involve <u>stakeholders</u> across the initiation, design, development, and operational stages.**

- **Focus on <u>accuracy and reliability, understandability, and transparency</u>.**

- **<u>Have guidelines to consider trade-offs</u> between principles, especially with respect to increasing transparency while preserving privacy, increasing accuracy while preserving fairness, and increasing accuracy while preserving understandability.**

- **<u>Maintain compliance</u> with relevant legal and regulatory authorities.**

- **<u>Have guidelines for the development, roll-out, use and evaluation</u> to address bias, identify chain of command, get and respond to stakeholder input, grievance procedure, test and address faulty outputs (model drift)**

- **<u>Maintain Active AI Governance Structures</u> that can guide Department-level policy and address gaps between guidance and application**

Questions? Ask ChatGPT (just kidding)

Paula Mallory Engel, Chief Welfare Attorney, Onondaga County

Telephone: 315-634-0504

Email: Paula.Engel@dfa.state.ny.us