



Moving AI Tools into Government: CDC Generative AI Guidance and Capabilities

Nadia FAWAZ, PhD

Presidential Innovation Fellow, CDC, Office of Science

05/02/2024 – AI Day for Federal Statistics: CNSTAT Public Event - NASEM

Generative AI

- Generating natural language (text and speech)

- Text completion: generate and edit text
- Embeddings: search, classify, and compare text

- Generating code

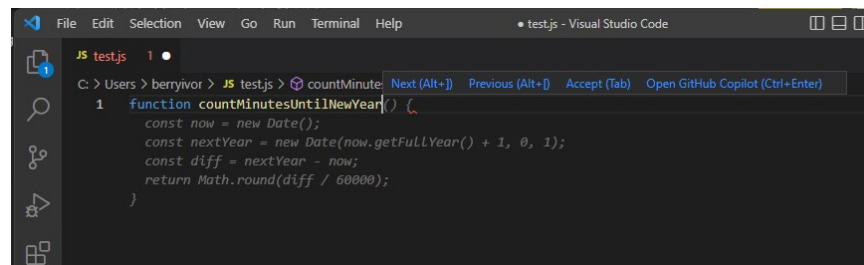
- Generate code from natural language or translate between programming languages
- Explain and debug code

- Generating images and videos

- Generate and edit images
- Embeddings: Search, classify, and compare images



Open AI. Introducing ChatGPT. <https://openai.com/blog/chatgpt>



<https://learn.microsoft.com/en-us/training/modules/explore-azure-openai/6-understand-openai-code-generation>



“A pink fox running through a field, in the style of Monet”, <https://learn.microsoft.com/en-us/training/modules/explore-azure-openai/7-understand-openai-image-generation>

AI \neq Generative AI

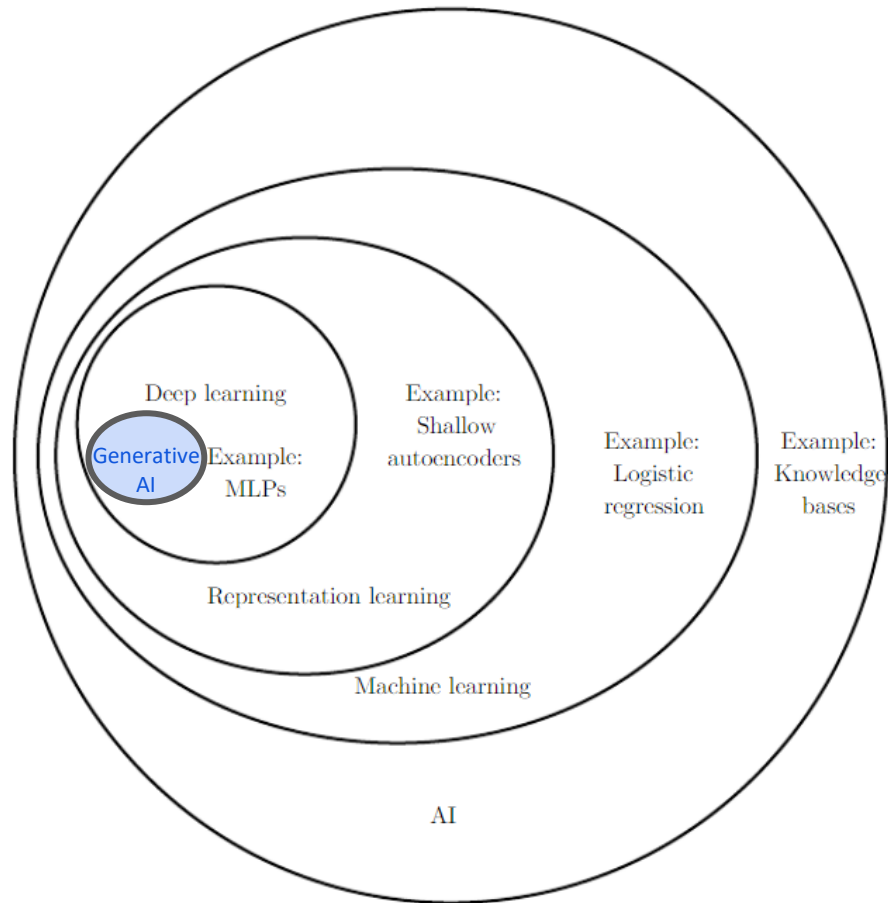


Figure 1.4: A Venn diagram showing how deep learning is a kind of representation learning, which is in turn a kind of machine learning, which is used for many but not all approaches to AI. Each section of the Venn diagram includes an example of an AI technology.

Serving the Public

[CDC's Vision](#): Equitably protecting health, safety, and security

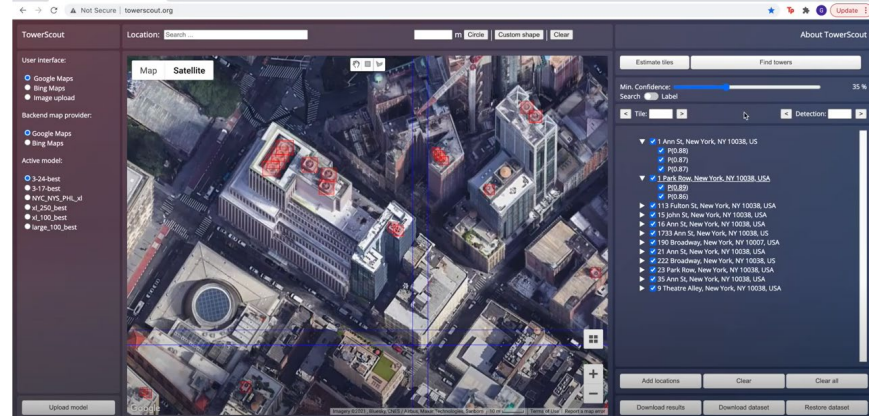
Computer Vision - HaMLET: Harnessing Machine Learning to Eliminate Tuberculosis

- At CDC, data scientists are exploring ways to use machine learning to leverage chest x-ray and tuberculosis data from overseas immigration visa screening examinations of immigrants and refugees to enhance programs to detect and treat tuberculosis (TB) to prevent TB importation.
- The computer vision model detects abnormal findings suggestive of TB in chest x-rays and can identify results that are discordant with the radiologist's findings.



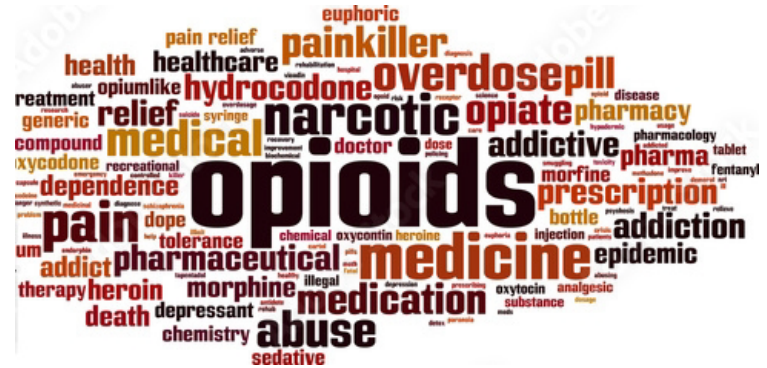
Computer Vision – TowerScout for Legionnaire's outbreak investigation

- Project: TowerScout Artificial Intelligence to Aid Outbreak Investigations Through the Identification of Cooling Towers Using Satellite Imagery
- The application allows someone to type in geographic identifiers for a Legionnaires' outbreak (e.g., zip code) and it returns a map image which displays identified towers as well as building addresses.
- This feeds satellite imagery into state-of-the-art machine learning algorithms that use computer vision technology to isolate cooling towers in those images.
- The application pings an Amazon Web Services machine which ingests the satellite images and maps from Bing Maps application programming interfaces (APIs) and runs them through the machine learning algorithm.
- <https://github.com/TowerScout/TowerScout>



Natural Language Processing – Detecting opioid use in clinical notes

- Named Entity Recognition for identifying opioid use in free text clinical notes from electronic health records
- Working with the National Hospital Care Survey to extract information on a patient's use of opioids from the free text in electronic health record (EHR) clinical notes
- Uses natural language processing (NLP) and named entity recognition to search for spelling variations of known opioids and determine whether their use is being affirmed or negated
- <https://www.cdc.gov/nchs/nhcs/index.htm>



Centers for Disease Control and Prevention
CDC 24/7: Saving Lives, Protecting People™



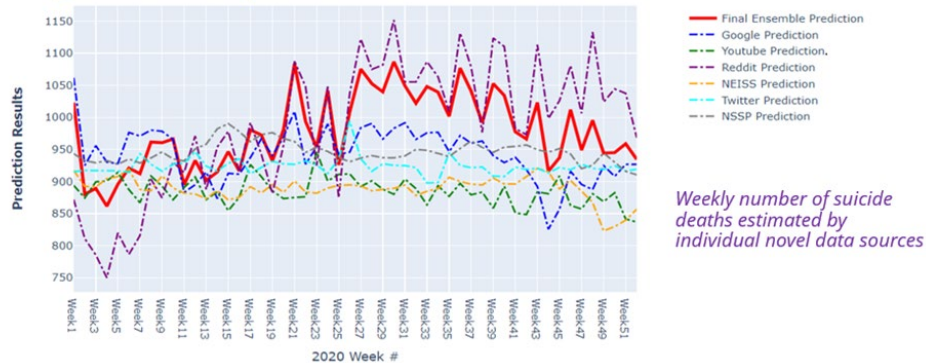
NHCSTM
National Hospital Care Survey

National Center for Health Statistics

RAPID: Machine Learning for “Nowcasting” Suicide Fatalities in the U.S.

- CDC’s National Center for Injury Prevention and Control has leveraged machine learning and artificial neural networks to integrate several streams of information to estimate weekly suicide fatalities in the U.S. in near real time.
- The ensemble machine learning framework reduces the error for suicide rate estimation, establishes a novel approach for tracking suicide fatalities in near real time, and provides the potential for an effective public health response and interventions to prevent suicides in the U.S.

Making Suicide Predictions from Data Sources



[Novel Approaches: "Nowcasting" Suicide Trends](#)
[| 2022 DMI Snapshot | CDC](#)

JAMA
Network | Open

Original Investigation | Health Informatics

Development of a Machine Learning Model Using Multiple, Heterogeneous Data Sources to Estimate Weekly US Suicide Fatalities

Daejin Choi, PhD; Steven A. Sumner, MD; Kristin M. Holland, PhD; John Draper, PhD; Sean Murphy, PhD; Daniel A. Bowen, MPH; Marissa Zwald, PhD; Jing Wang, MD; Royal Law, PhD; Jordan Taylor, BS; Chaitanya Konjeti, BS; Munmun De Choudhury, PhD

Abstract

IMPORTANCE Suicide is a leading cause of death in the US. However, official national statistics on suicide rates are delayed by 1 to 2 years, hampering evidence-based public health planning and decision-making.

Key Points

Question Can real-time streams of secondary information related to suicide be used to accurately estimate suicide fatalities in the US in real time?

<https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2774462>

Supporting CDC's staff

AI at CDC in Numbers

- 2 internal reports on CDC AI needs
 - 2022 Analytics and ML Implementation
 - 2023 Conversational AI
- 1,000+ attendees at Conversational AI 101 webinar in June 2023
- 1,400+ CDC AI Community of Practice members
- ~20 CDC public AI use cases in 2023 federal AI inventory (up 6x from 3 CDC public use cases in 2022)
<https://ai.gov/ai-use-cases/>
- 15+ use cases for 1st GenAI pilot initiative
- CDC AI intranet site with resources for staff (~10K views as of 4/23/2024)
- CDC's Guidance on Generative AI (1K+ downloads as of 4/23/2024)

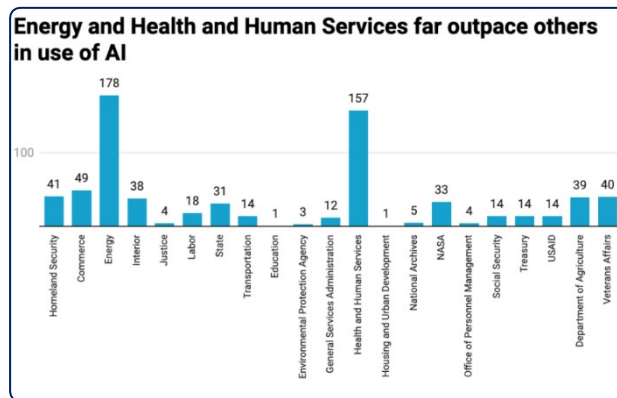


HHS's artificial intelligence use cases more than triple from previous year

The Department of Health and Human Services' annual AI use case inventory for fiscal 2023 includes 163 instances — up from 50 the previous year.

BY MADISON ALDER • AUGUST 15, 2023

<https://fedscoop.com/hhs-ai-use-casesmore-than-triple/>



<https://fedscoop.com/u-s-government-disclosesmore-than-700-ai-use-casesas-biden-administration-promises-regulation/>



U.S. government discloses more than 700 AI use cases as Biden administration promises regulation

The publication of the consolidated database of AI use cases in federal agencies comes as the Biden administration promises to beef up regulation of the technology.

BY MADISON ALDER AND REBECCA HEILWEIL • OCTOBER 13, 2023

<https://fedscoop.com/u-s-government-disclosesmore-than-700-ai-use-casesas-biden-administration-promises-regulation/>

CDC AI Road Map



Strategy



**AI Community of
Practice**



Guidance



Communication



**AI Consultation
Group (AICG)**



**Investments and
Infrastructure**



CDC AI Strategy

(Pre-decisional draft, work in progress, different from generative AI (GenAI) guidance)

Strategy 1: AI Adoption

Identify, develop, test, and implement AI technologies to solve complex public health problems and improve the health of the nation.

Strategy 2: Trustworthy AI

Ensure CDC develops and implements responsible and trustworthy AI that adheres to standards and best practices.

Strategy 3: Data and Technology

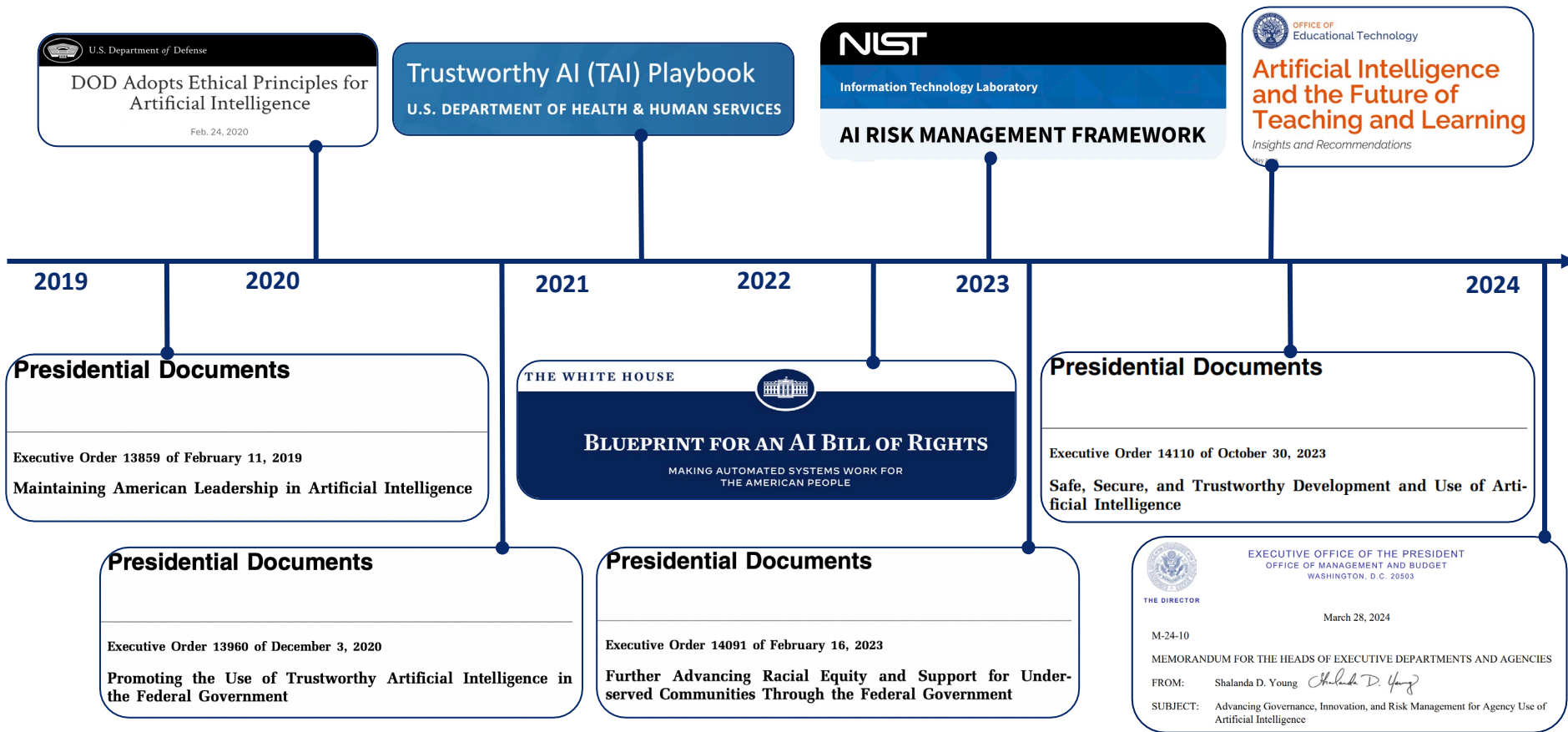
Invest in the AI-readiness of CDC and STLT data assets and the analytic, computing, and cloud technology needed to implement state-of-the-art AI technologies.

Strategy 4: Capacity-building

Increase CDC's capacity to implement AI technologies to improve public health outcomes through strategic partnerships and investments in human capital.

Delivering on Federal Priorities

Responsible AI initiatives in the Federal government



AI Executive Order (EO) 14110 and Office of Management and Budget (OMB) Memorandum M-24-10

EO 14110- 10.1.(f).(i) “As generative AI products become widely available and common in online platforms, **agencies are discouraged from imposing broad general bans or blocks on agency use of generative AI.** Agencies should **instead limit access as necessary to specific generative AI services** based on specific risk assessments, **establish guidelines and limitations on the appropriate use of generative AI;** and, with appropriate safeguards in place, **provide their personnel and programs with access to secure and reliable generative AI capabilities;** at least for the purposes of experimentation and routine tasks that carry a low risk of impacting Americans’ rights. To protect Federal Government information, agencies are also encouraged to **employ risk-management practices** such as **training their staff on proper use**, protection, dissemination, and disposition of Federal information; negotiating appropriate terms of service with vendors; **implementing measures designed to ensure compliance with record-keeping, cybersecurity, confidentiality, privacy, and data protection requirements** and deploying other measures to prevent misuse of Federal Government information in generative AI.”

EO 14110 - 10.1.(f).(ii) “Agency Chief Information Officers, Chief Information Security Officers, and authorizing officials are also encouraged to **prioritize generative AI** and other critical and emerging technologies in **granting authorities for agency operation of information technology systems** and any other applicable **release or oversight processes**, using continuous authorizations and approvals wherever feasible”

OMB Memo – 4.b.iv “**Generative AI.** In addition to following the guidance provided in Section 10.1(f) of Executive Order 14110, agencies should **assess potential beneficial uses** of generative AI in their missions and **establish adequate safeguards and oversight mechanisms** that allow generative AI to be used in the agency without posing undue risk.”

Generative AI Background

Potential Benefits and Risks of GenAI

Potential benefits	Potential risks	Potential threats by external actors
Increase efficiency: Accelerate manual or repetitive tasks that do not require a high level of expertise or that use structured formats	Failure to meet ethical or regulatory standards	Generating misinformation
Accelerate writing code	Fabrication, hallucinations	
Accelerate writing code	Plagiarism, copyrights violations	Impersonating agency
Synthesize and summarize information	Bias and discrimination	
Communicate: Adapt text to various reading levels, languages, platforms, audiences	Privacy and data security risks	Spamming agency
Personalize responses	Other legal or ethical risks, including risks to agency credibility	

Fabrications or “Hallucinations”

EM Can you please provide 5 scientific references for this information?

Certainly! Here are five scientific references related to mpox outbreaks and relevant topics:

1. Rimoin, A. W., Mulembakani, P. M., Johnston, S. C., Lloyd Smith, J. O., Kisalu, N. K., Kinkela, T. L., ... & Wolfe, N. D. (2010). Major increase in human monkeypox incidence 30 years after smallpox vaccination campaigns cease in the Democratic Republic of Congo. *Proceedings of the National Academy of Sciences*, 107(37), 16262-16267.
2. Likos, A. M., Sammons, S. A., Olson, V. A., Frace, A. M., Li, Y., Olsen-Rasmussen, M., ... & Reynolds, M. G. (2005). A tale of two clades: monkeypox viruses. *Journal of General Virology*, 86(10), 2661-2672.
3. McCollum, A. M., Nakazawa, Y., Loparev, V. N., Boyer, A. E., Reynolds, M. G., Damon, I. K., & Li, Y. (2014). The complete genome sequence of monkeypox virus West African clade. *Virology*, 474, 105-124.
4. Reed, K. D., Melski, J. W., Graham, M. B., Regnery, R. L., Sotir, M. J., Wegner, M. V., ... & Swain, G. R. (2004). The detection of monkeypox in humans in the Western Hemisphere. *New England Journal of Medicine*, 350(4), 342-350.
5. CDC. (2022). Monkeypox Cases Reported in the United States, 2022. Morbidity and Mortality Weekly Report, 71(32), 1089-1095. [This is a government report by the Centers for Disease Control and Prevention (CDC) that provides information on monkeypox cases reported in the United States.]

FACT

FACT

FACT

FICTION

FICTION

AI Risks

- Bias and inequity
- Lack of accessibility
- Errors, hallucinations
- Plagiarism, copyright violations
- Security vulnerabilities and privacy violations (PII, PHI)
- Lack of transparency
- Trust issues, closed boxes
- Lack of accountability, impact to rights

Responsible AI Principles

- Fairness, inclusion, equity
- Accessibility
- Safety, reliability, testing, evaluation, monitoring, human oversight
- Privacy and security
- Disclosure and transparency
- Explainability, interpretability
- Accountability, governance, ethical and legal standards

CDC GenAI Guidance and Capabilities

Process for Development, Subject Matter Expert (SME) and Clearance Review of GenAI Guidance

Development : cross-functional collaboration between Office of Science (OS), Office of the Chief Information Officer (OCIO), and Office of Public Health Data, Surveillance, and Technology (OPHDST) with contributions from multiple CDC Centers, Institutes, Offices (CIOs) and programs

Review

- ~500 comments by SMEs and clearance reviewers
- Clearance and SME reviews by leadership and CIOs

Briefings

- Internal to CDC
- Federal agencies working on GenAI guidance

GenAI Policies in Government...

...and in Journals

Federal policies/guidance

- **CDC**, Guidance on Generative AI, Feb. 6 2024 – internal
- **DHS**, Use of Commercial Generative Artificial Intelligence (AI) Tools, Oct. 24 2023 – publicly available [[dhs.gov](https://www.dhs.gov)]
- **DoD**, Establishment of Chief Digital and Artificial Intelligence Officer Generative Artificial Intelligence and Large Language Models Task Force, Task Force Lima, August 10, 2023 - publicly available [[defense.gov](https://www.defense.gov)]
- **GSA**, Security Policy for Generative Artificial Intelligence (AI) Large Language Models (LLMs) June 9, 2023 - publicly available [[gsa.gov](https://www.gsa.gov)]
- **NASA's** Use of Generative Artificial Intelligence (AI) Technologies, May 22, 2023 – publicly available [[sam.gov](https://www.nasa.gov)]
- **NIH** Office of Extramural Research. Use of Generative Artificial Intelligence Technologies is Prohibited for the NIH Peer Review Process. Notice number NOT-OD-23-149, June 23, 2023 - publicly available [[nih.gov](https://www.nih.gov)]
- **NIH** Frequently Asked Questions (FAQs) - Use of Generative AI in Peer Review. – publicly available [[nih.gov](https://www.nih.gov)]
- **NSF**, Notice to research community: Use of Generative artificial intelligence technology in the NSF merit review process, December 14, 2023 – publicly available [[nsf.gov](https://www.nsf.gov)]
- **USDA**, Interim Guidance on the Use of Generative Artificial Intelligence at USDA, October 16 2023 – publicly available [[fedscoop.com](https://www.fedscoop.com)]
- **VA** NAIL Information Bulletin on Generative AI Models, March 31, 2023 - internal

State policies: [California](#), [Kansas](#), [New Jersey](#), [Pennsylvania](#), [Washington](#)

City policies: [Boston](#), [San Jose](#), [Seattle](#)

Other Countries' GenAI Policies: [Canada](#), [UK](#)

- **MMWR**, CDC Morbidity and Mortality Weekly Report Instructions for Authors. Updated June 29, 2023. https://www.cdc.gov/mmwr/author_guide.html
- **ICMJE**. International Committee of Medical Journal Editors. Recommendations. Updated May 2023. <https://www.icmje.org/recommendations>
- **JAMA**. Editorial. Guidance for Authors, Peer Reviewers, and Editors on Use of AI, Language Models, and Chatbots. July 27, 2023. <https://jamanetwork.com/journals/jama/fullarticle/2807956>
- **JAMA**. Reporting Use of AI in Research and Scholarly Publication—JAMA Network Guidance. March 7, 2024. <https://jamanetwork.com/journals/jama/fullarticle/2816213>
- **Nature**. Editorial. Why Nature will not allow the use of generative AI in images and video. Nature. June 7, 2023. <https://www.nature.com/articles/d41586-023-01546-4>
- **NEJM AI**. Peer Review & Publication Process. <https://ai.nejm.org/about/publication-process>
- **NEJM AI**. Why We Support and Encourage the Use of Large Language Models in NEJM AI Submissions. December 11, 2023. <https://ai.nejm.org/doi/full/10.1056/Ale2300128>

CDC Guidance on Generative Artificial Intelligence

Internal CDC guidance covers

- Summary Recommendations
- Ethics and Scientific Integrity
- Generative AI Technology and Data: secure capabilities vs public interfaces
- Recommendations for Responsible Use and Development of GenAI
- Additional Practical Guidance for Specific Uses of GenAI
- Human Capacity
- Governance

Access types for GenAI

Public interfaces

Risks for security and privacy. These systems may reuse input prompts or data to train GenAI models and leak data to the public.

Examples

- OpenAI (web, APIs, mobile apps)
 - ChatGPT
 - DALL-E
- Google Bard/Gemini
- Anthropic Claude
- Microsoft BingChat
- Github Copilot

CDC secure enterprise system

These systems do not use input prompts or data, or generated outputs, to train, retrain, improve GenAI base models, or improve any provider or 3rd party's products or services.

Examples

- Microsoft Azure OpenAI service (web, API, AI search integration) – FedRAMP high
- Open-source GenAI models downloaded to CDC Azure data lake + Databricks (e.g., Meta Llama-2)

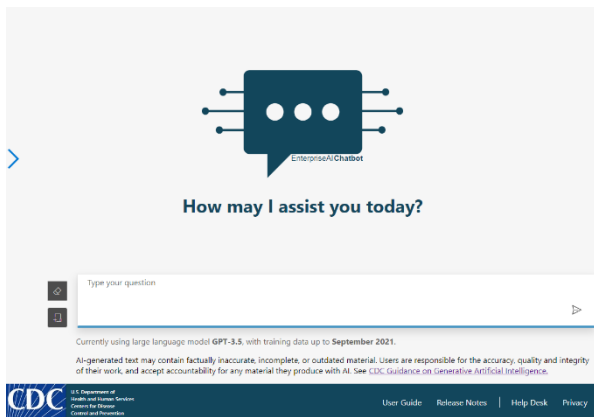
Other secure tools – not available at this time

- BingChat Enterprise, Windows Copilot, Microsoft 365 Copilot (not yet in government cloud, cost)

Secure GenAI Capabilities in Evaluation in CDC

Phased roll-out of capabilities: pilot testing preceding general availability

CDC secure enterprise chatbot
using Azure OpenAI



CDC general availability

CDC secure API
based on Azure OpenAI API

```
Python Copy

import os
from openai import AzureOpenAI

client = AzureOpenAI(
    azure_endpoint = os.getenv("AZURE_OPENAI_ENDPOINT"),
    api_key=os.getenv("AZURE_OPENAI_API_KEY"),
    api_version="2024-02-01"
)

response = client.chat.completions.create(
    model="gpt-35-turbo", # model = "deployment_name".
    messages=[
        {"role": "system", "content": "You are a helpful assistant."},
        {"role": "user", "content": "Does Azure OpenAI support customer managed keys?"},
        {"role": "assistant", "content": "Yes, customer managed keys are supported by Azure OpenAI."},
        {"role": "user", "content": "Do other Azure AI services support this too?"}
    ]
)

print(response.choices[0].message.content)
```

[Quickstart - Get started using GPT-35-Turbo and GPT-4 with Azure OpenAI Service - Azure OpenAI Service | Microsoft Learn](#)

CDC general availability

Integration with enterprise
data using Azure AI Search



In testing

General Guidance for Responsible Use and Development of GenAI



Additional Practical Guidance for Specific Uses of GenAI

- Operational Productivity and Communication Products
- Scientific Product Authors
- Scientific Product Reviewers
- Grants, Contracts, and Technology Transfer Agreements
- Software development
- Data Analysis

Do not list ChatGPT or other genAI technology as an author, nor cite AI as an author.

AI-generated code may contain bugs and may introduce security vulnerabilities. Staff should conduct proper code review and testing of AI-generated code prior to deploying the code in production.

GenAI Governance Section

- Roles and responsibilities for GenAI
- Criteria for GenAI governance review

GenAI Pilots

GenAI Pilots Overview

- 15 generative AI pilots (7 CIOs) initiated in November 2023
- Established tight feedback loop between pilots, tech team, leadership, and governance/policy.
- Use cases ranged from **public health research, operational efficiency, and communications.**

Pilot: Information Extraction

Insights from Older Adult Falls in Emergency Dept Narratives

Input: You are a public health expert on fall injury.

What is the patient's activities right before the fall injury. Please provide the answer directly. If there is no answer just say 'None'.

Narrative	Activity
94YOM FELL TO THE FLOOR AT THE NURSING HOME ONTO BACK OF HEAD SUSTAINED A SUBDURAL HEMATOMA	None.
86YOM FELL IN THE SHOWER AT HOME AND SUSTAINED A CLOSED HEAD INJURY	Showering at home.
87YOF WAS GETTING UP FROM THE COUCH AND FELL TO THE FLOOR SUSTAINED ABRASIONS TO ELBOWS ADMITTED FOR HEMORRHAGIC STROKE	Getting up from the couch
67YOF WAS AT A FRIENDS HOUSE AND SLIPPED ON WATER THAT WAS ON THE FLOOR AND SUSTAINED A RIGHT RADIUS FX	The patient slipped on water that was on the floor at a friend's house.
70YOF WAS STANDING ON A STEP STOOL AND FELL OFF SUSTAINED A RIGHT RADIUS FX	Activities right before the fall injury: Standing on a step stool.

Results: Tested on 15 examples. 100% accuracy based on manual review.

Pilot: Facilitate Review of Public Comments

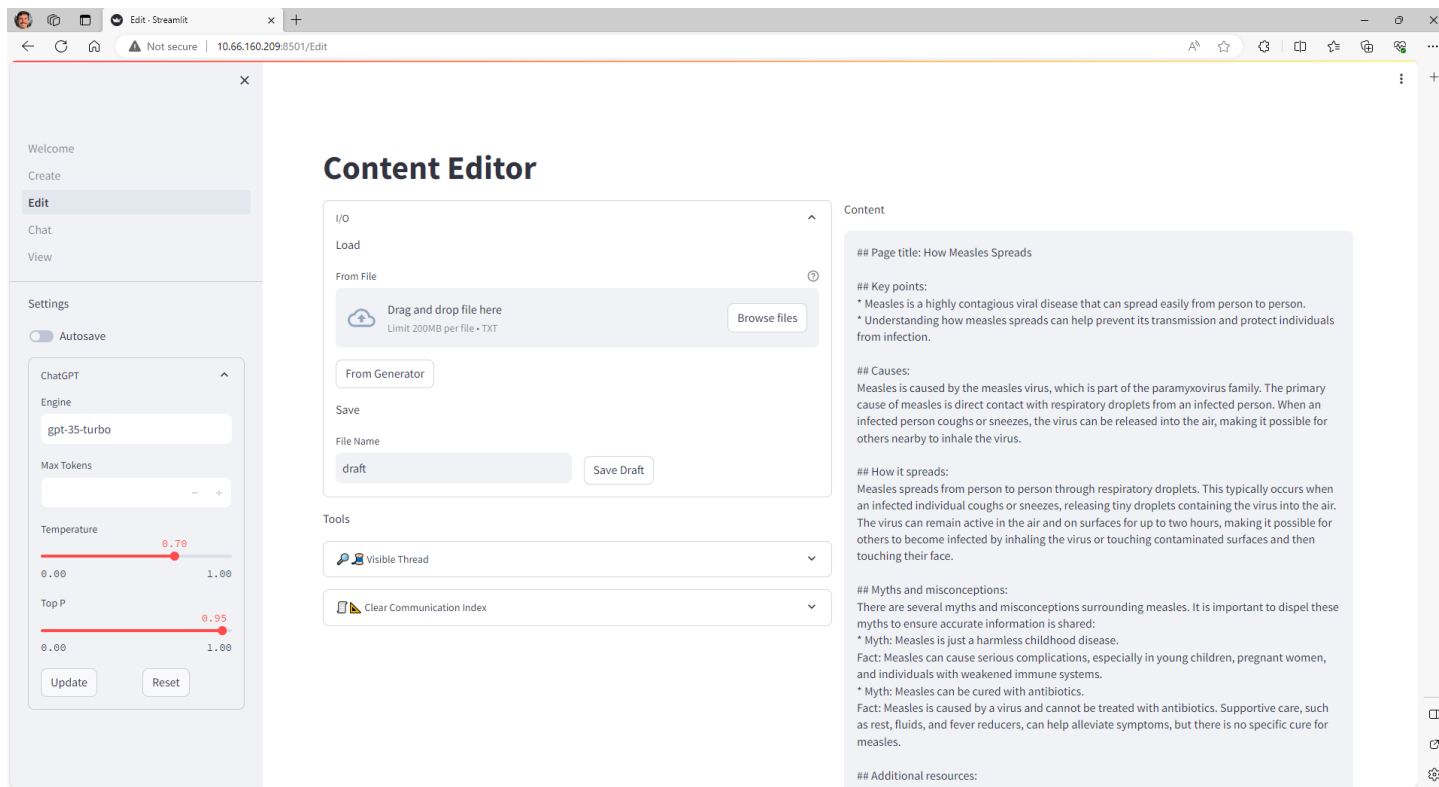
Generative AI for Stance Analysis of Public Comments on CDC's Proposed Rules

- Regulations.gov enables the public to comment on new proposed rules
- Natural Language Processing can *accelerate* (not replace) manual review by identifying common themes/topics and sentiment analysis
- GenAI showed promise (77% accuracy on 435 comments) in identifying comment stance
- Possible values: SUPPORT, OPPOSE, UNCLEAR

ID	Text	Manually labeled stance	Automatically labeled stance	GenAI Reasoning
Numeric ID	PROBLEMATIC MAJOR OVERSIGHT: In the proposed new regulations, there is no accounting for those of us ALREADY/currently abroad in a DMRVV High-Risk Country with a pet with a valid US-issued rabies vaccination certificate (US RVC). This applies to thousands of US government personnel abroad. We are not able to obtain a "Valid Certification of U.S.-issued Rabies Vaccination for Live Dog Re-entry into the United States form PRIOR to the dog's departing the United States" as required because we are ALREADY abroad with our dog. The proposed regulations provide no instructions to those of us in this situation (dog already abroad + valid RVC) and the other scenarios in the proposed regulations do not apply. We would not qualify for a CDC import	Oppose	Oppose	The commenter is objecting to the proposed notice <i>due to lack of clarity and provisions for those who are already abroad in a DMRVV High-Risk Country with a pet that has a valid US-issued rabies vaccination certificate. They propose that a digital certification process or a waiver for a one-year period should be implemented, hence they are against the notice in its current form.</i>

Pilot: Preliminary User Interface (UI) for Web Content Creation and Editing

Clear Language for Clean Slate



Questions?

For more information, contact CDC/ATSDR

1-800-CDC-INFO (232-4636)

TTY: 1-888-232-6348 www.cdc.gov www.atsdr.cdc.gov

The findings and conclusions in this report are those of the authors and do not necessarily represent the official position of the Centers for Disease Control and Prevention and the Agency for Toxic Substances and Disease Registry.



ATSDR