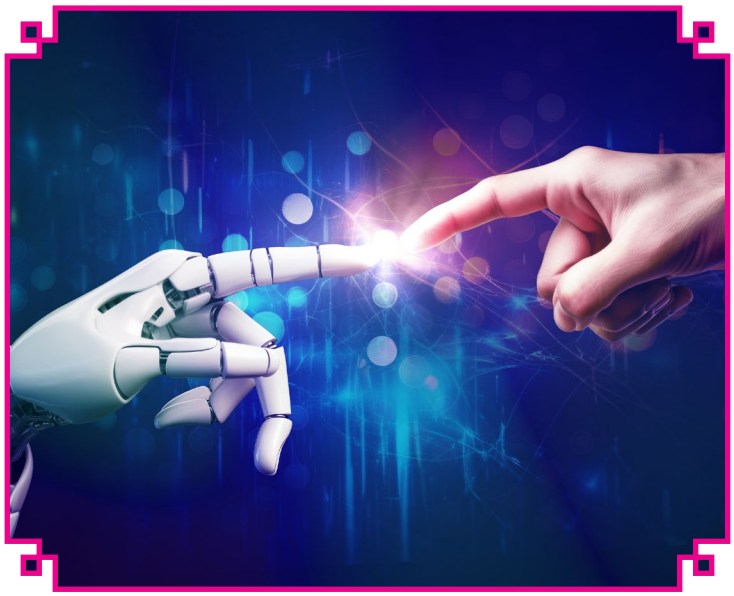
AI Tools for HHS

How to Get Started at IHS

Office of Information Technology
Division of Information Security
MARCH 2026

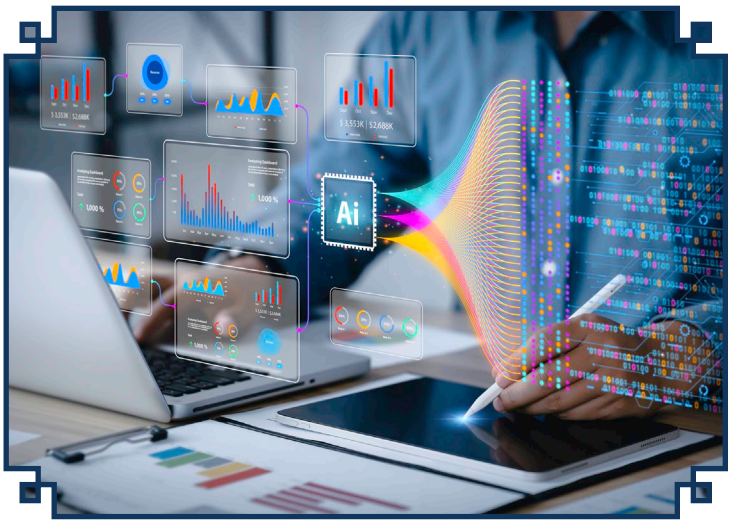
Artificial Intelligence (AI) has become increasingly popular, changing the way people approach their work. AI tools such as automated assistants, chat logs, and image creators play an increasing role in the workflows of today's positions.



While AI has become popular in the last few years, the use of artificial intelligence can be traced back to the 1960s. The invention of the ELIZA chatbot in 1964 started the study of communication with machines through its natural language processing. Generative AI technologies – AI systems with the ability to produce unique outputs based on user prompts – have become popular in the last decade. Millions of people around the world have used generative AI systems to produce a variety of outputs, from text to computer code to videos.

Health and Human Services (HHS) is the first Federal government agency to allow the use of generative AI at all levels of the organization. The AI Action Plan, a set of Executive Orders signed in July 2025, seeks to increase the use of AI in America. This initiative is focused on three pillars of action: accelerating innovation, building infrastructure, and leading international diplomacy and security.

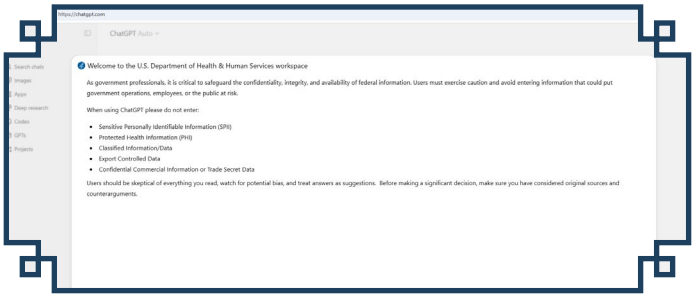
Two generative AI models have been cleared for daily use at HHS: ChatGPT and Gemini. Both models are Federal Risk and Authorization Management Program (FedRAMP) High-authorized environments, meaning that they have the highest level of security possible for a cloud-based system used in the federal government. Both ChatGPT and Gemini can safely be used on sensitive data but are not approved for disclosure of personally identifiable information (such as social security numbers) or protected health information (such as patient records) in accordance with Health Insurance Portability and Accountability Act of 1996 (HIPAA) rules. These AI instances also cannot be used with classified information, export-controlled data, or confidential commercial information subject to the Trade Secrets Act. Within these limits, users can work confidently and securely while maintaining full compliance with federal cybersecurity and privacy standards.



To access these protected instances of ChatGPT and Gemini, users must use the following links:

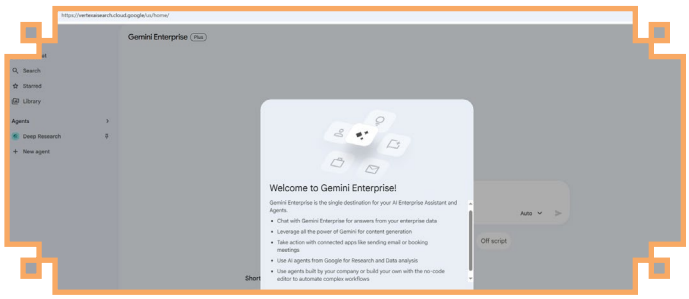
Do not access AI tools outside of these URLs.

To use ChatGPT, visit https://go.hhs.gov/chatgpt



To use Gemini, visit https://go.hhs.gov/gemini

Training for Gemini is available at the following URL: https://www.skills.google/paths/2919



As a healthcare delivery organization, Indian Health Services (IHS) is under constant threat from bad actors trying to access confidential information. With the popularity of AI tools and the rollout of their use at HHS, cybercriminals may attempt to trick users into using an unauthorized instance of ChatGPT or Gemini through phishing emails or other communications that mimic official channels. To prevent this, bookmark the URLs provided above and only access the tools through those bookmarks. If you receive an email or other communication trying to get you to click on a link to an AI tool, report it to the Cybersecurity Operations Center (CSOC) by emailing incident@ihs.gov.

While generative AI can help with productivity, it is not without flaws. While using this technology, be on the lookout for information that seems inaccurate or biased. Generative AI has been known to “hallucinate” and give false information sometimes. Question information generated using AI. It is your responsibility to ensure that work is accurate and complete, whether using these tools or not.

Artificial intelligence is a cutting-edge tool that can help with productivity and accessibility. When using AI at work, always access tools through the proper websites and be cognizant of the types of information you enter into them. Check your work and be vigilant for errors or bias.

NOTE: The links in this document are for informational purposes only, and do not signify an endorsement of any products contained within the linked sites/files.

Please contact cybersecurity@ihs.gov with any questions or comments about this newsletter.