STATE OF UTAH
OFFICE OF THE UTAH STATE AUDITOR

TINA M. CANNON
UTAH STATE AUDITOR

Comment Period: In an effort to make our publications accurate and useful to our intended audience, we invite individuals who work for and with government entities to read this draft and provide comment. The comment period will end September 7, 2025. Comments should be submitted to Nora Kurzova at nkurzova@utah.gov.

Privacy Alert 2025–03 - DRAFT

Date: August 7, 2025

Subject: Artificial Intelligence (AI) May Not Keep Your Secrets

Generative AI systems are types of AI that are designed to create content, such as images, text, code, or music based on what it has learned from existing data. Examples would include ChatGPT, Gemini, Claude, and others. While using generative AI systems offers fast responses and often impressive results, using them in a work setting comes with data security, privacy, and reliability concerns. Below are three points every user should understand before using generative AI tools in their work.

Deleting Data Does Not Always Mean It Is Gone

Even if a Generative AI tool claims to delete inputs upon your request, your data may still be stored somewhere or be recoverable in other ways:

1. **Court orders or subpoenas** may compel providers to retain and disclose data
2. **Caching and backup systems** may preserve interactions beyond your session
3. **Model training** may use your data unless strict opt-out settings or enterprise controls are in place and are configured and used correctly

The best policy is to never enter sensitive, confidential, or regulated data, even temporarily, into any AI tool that you do not fully control. You should also understand users may sometimes be identifiable indirectly through the content of their chats and prompts they give the tool.

New Risks Arising from Public Indexing

Some ChatGPT conversations, specifically those shared using the platform's "Share Chat" feature, may have been previously indexed by search engines like Google. This means that some user prompts, as well as the AI generated responses, became publicly searchable online prior to August 1, 2025.

While indexing and the option to make shared chats publicly discoverable may have been disabled by Google and OpenAI as a follow up to the public concern[1] expressed in the media globally[2], many of the previously shared chats are still discoverable online.

This underscores an important risk: Any AI tool that allows sharing or saving content externally may increase the chance of unintentional unlimited disclosure, if not properly configured or used.

AI Is Not a Neutral Party, Expert, or Professional Advisor

Generative AI tools do not understand the truth or always interpret context correctly. They generate output based on patterns in data and can provide false or misleading results. They should not be relied on for **legal, medical, forensic, or mental health** decisions and human oversight should be a critical part of working with generative AI.

However, if a user themselves lacks deep understanding of the topic they are working on, they may not catch incorrect or incomplete outputs. This creates risks when AI is used for tasks that require accuracy, fairness, or checking for compliance.

Bottom Line:

Treat Generative AI tools like any other third-party service:

- Don't input sensitive or confidential data.
- Don't rely on Generative AI for expert advice.
- Train your users on proper uses of generative AI and its limitations.
- Create and disseminate a policy on proper use of AI within your organization.

Call to Action:

To request an audit of how a particular governmental entity uses generative AI or for more information, contact the State Privacy Auditor at privacy@utah.gov

[1] https://www.lifewire.com/google-indexed-chatgpt-conversations-11784115

[2] https://www.computing.co.uk/news/2025/ai/thousands-of-chatgpt-conversations-appear-in-google-results https://www.techradar.com/ai-platforms-assistants/chatgpt/openai-pulls-chat-sharing-tool-after-google-search-privacy-scare