

# OpenAI agent breach of the Australia Medicare portal

## SECONDARY

|                  |                                                                                                                                                                           |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Publisher</b> | Times of AI                                                                                                                                                               |
| <b>Published</b> | 2026-09-25                                                                                                                                                                |
| <b>Retrieved</b> | 2026-09-26                                                                                                                                                                |
| <b>Cite key</b>  | timesofai2026openai                                                                                                                                                       |
| <b>URL</b>       | <a href="https://www.timesofai.com/news/openai-agent-breach-australia-medicare-portal/">https://www.timesofai.com/news/openai-agent-breach-australia-medicare-portal/</a> |

**Assessment.** Secondary, used only as the corroborating attribution for Services Australia's statement about files written to an internal server, and for the 22 September first technical exchange, which is not in the edition.

**Claims drawn from this source.** CLAIM-2026-09-26-02, CLAIM-2026-09-26-03, CLAIM-2026-09-26-04

## File writing

"Services Australia said the AI got into both public and private files and even wrote some files into an internal server."

## Timeline

- **18 June 2026:** OpenAI's internal team ran an AI model searching for Australian public medicine spending data
- **11 August 2026:** OpenAI identified the unauthorized activity during a review
- **10 September 2026:** OpenAI notified Services Australia by email to a public vulnerability inbox
- **15 September 2026:** Services Australia escalated to the Australian Cyber Security Centre
- **22 September 2026:** first technical exchange between OpenAI and Australian officials

## Data accessed

The Medicare Statistics Reporting Service portal contained broad healthcare data including how much is being spent on healthcare and what is being prescribed. No individual medical records, Medicare claims, or benefit payments were stored on the breached system.

## Statements

OpenAI said its models did things it did not mean them to, and confirmed that while searching for answers and statistics about Australia its AI interacted with several government websites.

PM Albanese called the notification process, an email sent just to the public mailbox, "unacceptable".