

NHS to close-source hundreds of GitHub repos over AI, security concerns

Healthcare giant's maintainers handed May deadline to enact the change

Connor Jones

Tue 5 May 2026 // 09:15 UTC

The UK's National Health Service (NHS) is ordering all of its technology leaders to temporarily wall off the organization's open source projects over concerns relating to advanced AI and Anthropic's Mythos.

According to guidance shared internally within the organization and seen by *The Register*, GitHub repositories must be set from public to private by May 11.

The guidance reads: "Public repositories materially increase the risk of unintended disclosure of source code, architectural decisions, configuration detail, and contextual information that may be exploited – particularly given rapid advancements in AI models capable of large-scale code ingestion, inference, and reasoning (e.g. developments such as the Mythos model)."

It also states GitHub repos should not be public "unless there is an explicit and exceptional need." The decision was approved by the NHS' Engineering Board.

An NHS England spokesperson told *The Register* this was merely a temporary measure enacted while the organization shores up its cybersecurity posture.

"We are temporarily restricting access to some NHS England source code to further strengthen cybersecurity while we assess the impact of rapid developments in AI models," they said.

"We will continue to publish source code where there is a clear need."

NHS sources told us very few of the hundreds of NHS open source repositories contain anything remotely sensitive. Examples of open repos include those dedicated to documentation, architecture diagrams, and codebases for internal tools, such as web apps for managing clinic times.

While there are bugs that a frontier AI model such as Mythos could unearth, there is thought to be very little risk to healthcare services.

The NHS's decision to pull a curtain over its code *does*, however, mark a significant, albeit temporary, U-turn in its longstanding policy of favoring open source.

Reflecting the [policy of the wider British government](#), the organization's [service manual](#) states that all new source code should be made open source and shareable under an appropriate license. Its reasoning lies in how it is funded.

"Public services are built with public money," the manual states. "So unless there's a good reason not to, the code they're based [on] should be made available for other people to reuse and build on."

"Open source code can save teams duplicating effort and help them build better services faster. And publishing source code under an open license means that you're less likely to get locked in to working with a single supplier."

Reports on the NHS [deleting web pages](#) devoted to communicating its approach to open source circulated late last year, suggesting it could be wavering.

However, the healthcare org responded by saying this was part of a routine cleanup job related to [NHSX and NHS Digital being folded into NHS England](#).

MORE CONTEXT

[Usage-based pricing killing your vibe - here's how to roll your own local AI coding agents](#)

[Microsoft fixes VS Code after app gives Copilot credit for human's work](#)

[Mythos complicates the breakup, says Pentagon CTO, but Anthropic is still barred](#)

[Zed team releases version 1.0 of Rust-built editor: Traditional editor and AI tool](#)

NHS England did not give an estimate for when this temporary closed-sourcing will end, nor did it answer questions about what it deems the most significant threats advanced AI models pose to its open source repos.

Mythos... threat or fud?

Reg readers have no doubt caught the ghost stories swirling around Anthropic's latest AI model, Mythos. It is touted by Anthropic as a model capable of rapidly finding vulnerabilities that skilled human teams would miss. Others see it as over-hyped.

National authorities, including the UK's AI Safety Institute and National Cyber Security Centre, have somewhat validated Anthropic's claims of Mythos representing an advancement beyond the forecasted AI development cycle.

However, others are more [sceptical](#) about the [purported bug-hunting power](#). Anthropic has still not yet revealed the number of false positives the model throws up when running vulnerability scans, which is a common issue with AI thus far.

Tests comparing Mythos with open source models have also revealed the [proficiency gap](#) is narrower than Anthropic implies.

For now, Mythos is locked behind Project Glasswing, available only to select organizations. But [Forrester analysts warn](#) that once powerful models reach the public - and attackers - open source software faces a genuine threat, one that could be addressed by AI. [Open source software](#) is a [recent blog](#).

Former head of open source at NHS, he said, "People's open source code is in a [recent blog](#). If it was moderate, various digital libraries, and so on. Closing now does not mean it's gone. Many of the serious codebases, he added, are in private repositories, and so on. The bigger risk comes from the fact that some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page or in the site menu to manage or withdraw consent in privacy and cookie settings.

"The bigger risk comes from the fact that some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page or in the site menu to manage or withdraw consent in privacy and cookie settings."

No more fake tech

MORE ABOUT

[Anthropic](#) [Exclusive](#) [NHS](#) [More like these](#)

TIP US OFF

[Send us news](#)

DIY mystery box will wow your friends by hinting at what the ionosphere is up to
A rough guide to when your signal will behave, or not
OFFBEAT Just posted | 1

Attackers are cashing in on fresh 'CopyFail' Linux flaw
Researchers dropped a reliable root exploit and it didn't sit idle for long
CYBER-CRIME 1 hr | 4

More missions, less money, higher risk: NASA's back to the '90s playbook
Faster, better, cheaper is back and history suggests you can't get all three at the same time
SCIENCE 2 hrs | 4

NeuBird AI plans a bright future for incident response
Imagine an army of AI minions handling investigations behind the scenes
SPONSORED FEAT...

17 COMMENTS

Bun posts Rust porting guide, says rewrite is still half-baked
Zig's no-AI policy is at odds with view that most open source code will be AI-written in future
DEVOPS 3 hrs | 1

Real estate giant confirms vishing incident as ShinyHunters and Qilin both come knocking
Cushman & Wakefield activated incident response protocols after serial extortionists issued separate threats
CYBER-CRIME 3 hrs | 1

SAP dives deeper into iceberg with Dremio acquisition
ERP giant previously leaned on Databricks for integration
DATABASES 3 hrs | 1

VMware claims Cloud Foundation on track for world domination
Delivers update aimed at reducing hardware bill shock
PAAS + IAAS 4 hrs | 1

ShinyHunters claims dump puts 119K Vimeo emails in the wild
Vimeo points finger at analytics supplier Anodot, says no logins or card data were touched
CYBER-CRIME 5 hrs | 4

Brit mathematician lets AI agent loose with credit card – cue password leaks, CAPTCHA chaos and more
Professor Fry's AI experiment shows light and dark sides of agentic tech
AI + ML 5 hrs | 33


Romance scammers turn sweet talk into £102M payday
Victims losing £280K a day to fake profiles and sob stories
SECURITY 5 hrs | 2


Vodafone dials up full control of joint venture with Three in £4.3B deal
CK Hutchison takes early cash as UK mobile tie-up moves ahead of schedule
NETWORKS 5 hrs | 8



The Register®

The Register asks for your consent to use your personal data to:

 Personalised advertising and content, advertising and content measurement, audience research and services development

 Store and/or access information on a device

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with 220 partners, or used specifically by this site. We and our partners may use precise geolocation data. [List of partners.](#)

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page or in the site menu to manage or withdraw consent in privacy and cookie settings.