

Major Medical Records Firm Uses A.I. Tool and Finds Flaws That Threaten Patient Privacy

Epic's engineers deployed an Anthropic tool that exposed security risks that could allow undetected access to millions of patient records.

By [Christopher Rowland](#) the New York Times

Sept. 30, 2026

Epic Systems, the nation's largest medical records vendor that is relied on by thousands of hospitals and doctors' offices, is using artificial intelligence tools to patch security risks that could give hackers undetectable access to patient health data, company officials said.

The unusual nature of the vulnerability and the urgency to fix it prompted Epic to slow down development of some product lines while it sent engineers into a sprint to patch security holes.

Judy Faulkner, Epic's chief executive, revealed the security weakness and a six-week plan to shore up the gaps at an industry conference last week, but most details about the danger have not previously been reported.

"You worry that after a month and a half of working almost primarily on safeguarding the software, that new things will be created by those who are trying to bust the software, and it will be in a never-ending cycle," [Ms. Faulkner said](#).

According to company representatives, Epic deployed Anthropic's Claude Mythos artificial intelligence agent to stress-test its systems, to hunt for ways that hackers could unleash open-source A.I. agents and unlock confidential patient records.

The security weaknesses pose a particularly acute threat for Epic, which maintains records of 325 million patients in the United States and other countries.

And it underscores the competing forces surrounding the ever-expanding uses of artificial intelligence in health care.

Like other companies, Epic is developing intelligent tools to help hospitals, doctors and researchers use patient records to make better decisions and analyze medical data. On the other side, hackers, who for years have been stalking hospitals in extortionate schemes, are employing A.I. in an accelerating cybersecurity arms race.

In addition, Epic has been dealing with a phishing scam by outside hackers that targeted users of the company's very popular MyChart portal, which allows patients to communicate with doctors and review their tests.

Health networks were the most frequently targeted in 2025 of all sectors considered critical to the United States, according to F.B.I. data, with 460 ransomware attacks and 182 data breaches.

One of the most recent hacks involved OpenAI, [which apologized](#) Tuesday after its A.I. agents gained unauthorized access to Australian government programs, including the universal health insurance system that covers most of the country's citizens. The authorities there said they were not notified of the breach until three months after the June breach. The agents did not get into the records of individual patients, according to a statement from OpenAI.

In the United States, [a ransomware attack](#) two years ago froze the systems of the health care billing and payment company Change Healthcare, which is owned by UnitedHealth Group. The episode paralyzed back-office operations in hospitals across the country while [highlighting the dangers](#) of having a single company responsible for keeping afloat such a large swath of the health care economy. Months later, Change Healthcare advised the federal government that the breach affected 190 million people and that it sent 130 million notices to patients that their records may have been stolen.

Using Mythos, Epic learned in recent months that certain configurations of software might permit someone to see sensitive patient records without the intrusion being reflected in a digital audit trail, Stirling Martin, Epic's senior vice president and chief security officer, said in an interview.

Although Mythos did not determine whether a hacker could take the next step and alter records, the test nonetheless raised such a possibility, Mr. Martin said.

"Whether things can be changed is more complicated, and depends on other parts of the technology and not necessarily Epic's in that case," Mr. Martin said.

Unless defenses are built to withstand such an incident, entering and changing patient records would represent a dangerous new frontier in medical information attacks, cybersecurity experts said.

Ransomware strikes typically shut down patient records systems as part of an extortion scheme. Other breaches involve the theft of large volumes of records that are sold on the dark web. Altering medical records could escalate the security threat to a new level and endanger lives, if, for example, data about a patient's penicillin allergy were erased.

This type of scheme — called an "integrity" attack — would rattle confidence in digital health systems, said Kevin Fu, a professor and director of the Archimedes Center for Healthcare and Medical Device Cybersecurity at Northeastern University.

A security flaw in which a criminal "could not only tamper with electronic health records, but also wipe away the trail — that is the exact opposite of integrity," Mr. Fu said.

Jackie Mattingly, who advises community hospitals as a senior director at Clearwater, a health cybersecurity firm, said A.I. was rapidly enhancing the capability of hackers hunting for vulnerable health care institutions.

"It's helping attackers move through the attack process much faster," Ms. Mattingly said. "It's helping them run the existing playbooks they already used at greater scale and with less expertise."

Ms. Faulkner, who founded the privately held Wisconsin-based company [in her basement](#) in 1979, said last week at a conference sponsored by the publication Modern Healthcare that Epic had uncovered new security gaps. She [was quoted](#) as saying most new product development had been paused to take care of fixes. The company later clarified that its new products remained on track.

Mr. Martin, Epic's chief of security, said rapidly evolving threats required health systems to be at the top of their game as medical record companies raced to stay ahead of hackers.

"Ultimately they need to get ready to patch, patch, patch," he said. "As soon as they think they are patching fast enough, they need to patch faster."

Epic's defensive upgrades are occurring alongside warnings about the MyChart attacks, a problem the company has little power to control.

Criminals are using basic A.I. tools to make highly realistic fakes of MyChart emails that advise people they are eligible for a free "Medicare Kit" or that purport to be conveying urgent test readings, said John Riggi, a longtime former F.B.I. cybersecurity specialist who is now a national cybersecurity adviser for the American Hospital Association.

These scams are mostly aimed at persuading patients to enter credit card numbers or MyChart security credentials. Epic and its client health systems have been warning patients for the past month not to be fooled and to avoid clicking on any email links. They should access their health records only through the MyChart app.

“What used to be email phishing — they were almost quaint. You could identify it through misspellings and so forth,” Mr. Riggi said. “Now, A.I. is producing highly convincing, perfectly worded emails, using personal health information in combination with voice calls, which layer credibility and complexity to the scheme.”