

**Statement
of the
American Hospital Association
for the
Committee on Homeland Security and Governmental Affairs
Subcommittee on Disaster Management, District of Columbia and Census
U.S. Senate
“Rogue AI: Securing the Homeland Against AI Agent Attacks”
September 30, 2026**

On behalf of AHA’s nearly 5,000 member hospitals, health systems and other healthcare organizations, our clinician partners — including more than 270,000 affiliated physicians, 2 million nurses and other caregivers — and the 43,000 healthcare leaders who belong to our professional membership groups, the American Hospital Association (AHA) writes to you in advance of the September 30 hearing, “Rogue AI: Securing the Homeland Against AI Agent Attacks.” We appreciate the committee’s focus on this important issue as cyberattacks continue to rise, causing impacts for patients, hospitals and health systems, and the entire healthcare sector.

Hospitals and Health Systems are Committed to Cybersecurity

Cybersecurity is critical to ensuring that hospitals can provide safe, high-quality care to their communities. Hospitals and health systems have invested billions of dollars and taken many steps to protect patients and defend their networks from cyberattacks that can disrupt patient care and erode privacy through the loss of personal healthcare data. The AHA has long been committed to helping hospitals and health systems with these efforts, working closely with our federal partners, including the Federal Bureau of Investigation (FBI), the Department of Health and Human Services (HHS), the Cybersecurity and Infrastructure Security Agency and many others to prevent and mitigate cyberattacks.



As data theft and ransomware attacks targeting healthcare have increased dramatically over the past several years, the AHA has worked closely with federal agencies and the hospital field to build trusted relationships and channels for the mutual exchange of cyber threat information, risk mitigation practices and resources to implement these practices. The AHA's work in this area is critically important and has allowed us to quickly assist members in their response to cyberattacks, including the [Change Healthcare cyberattack in 2024](#).

Rise of Cyberattacks and AI Impact

Cyberattacks against healthcare continue to grow in frequency, sophistication and impact. In recent months, there has been a troubling increase in cyber threats perpetrated by international cyber gangs and state-sponsored hackers. They have increased their targeting of healthcare third-party vendors, conducted ransomware attacks and led data-theft extortion campaigns. In 2025, the FBI reported that the healthcare sector [suffered more ransomware attacks](#) than any other critical infrastructure sector: There were 460 reported attacks, compared to 355 attacks against the next most attacked sector, critical manufacturing. The situation is [only getting worse](#) as nation-states and criminal hackers begin to use artificial intelligence (AI) to quickly identify software vulnerabilities and to rapidly develop and deploy malware to exploit weaknesses.

Attacks on third-party vendors, utilities and supply chain partners have demonstrated that an organization's cybersecurity posture is only as strong as the ecosystem on which it depends. In February 2024, [Change Healthcare](#), a subsidiary of UnitedHealth Group, was the victim of a ransomware attack by the Russian ransomware gang known as BlackCat or ALPHV. Change Healthcare, which processes [15 billion healthcare transactions annually](#) and touches 1 in every 3 patient records, would become the epicenter of the most consequential cyberattack on the U.S. healthcare system in history, causing significant disruptions to patient care and hospital finances that lasted for months. In this attack alone, the healthcare records of more than [192 million Americans](#) were stolen.

While AI holds tremendous promise to drive efficiencies and enhance quality of care, it also has the potential to introduce unique cybersecurity vulnerabilities. AI systems rely on large data sets to maximize their predictive power. However, aggregating large data sets also may pose unique cybersecurity risks that can further be exposed by privacy and security standards gaps. With the rise in third-party vendor protected health information (PHI) data breaches, it is essential entities that hold or process PHI (including certain AI vendors that may not meet the definition for covered entities or business associates under the current law) and are not currently covered by HIPAA, be subject to similarly rigorous privacy and security standards.

Government Response to Cyberattacks

To make meaningful progress in the war on cybercrime, Congress and the Administration must focus on the entire healthcare sector. According to the [HHS Office for Civil Rights](#) (OCR), the number of individuals impacted by healthcare data breaches increased from 27 million in 2020 to a staggering 259 million in 2024. Hospitals and health systems are not the primary source of cyber risk exposure facing the healthcare sector. Most PHI data breaches reported to OCR were the result of hacking incidents targeting non-hospital healthcare providers and third-party service and software providers. We believe third parties handling health information should be held to the same privacy and security standards as covered entities and business associates.

Hospitals' efforts alone are not enough to defend against nation-state-level cyberattacks. Congress should call on federal agencies to protect hospitals and health systems — and the patients they care for — by deploying a strong and sustained offensive cyber strategy to combat this ongoing and unresolved national security threat. The FBI's current aggressive offensive cyber campaign, known as [Operation Riptide](#), is an excellent example of this concept, as it has resulted in the dismantling of certain hackers' technical infrastructure, seizure of illicit proceeds, and a number of hacker arrests and extraditions to the United States.

Healthcare is a top critical infrastructure sector with direct impact on public health and safety, and it must be protected. Any cyberattack on the healthcare sector that disrupts or delays patient care creates a risk to patient safety and crosses the line from an economic crime to a threat-to-life crime. These attacks should be aggressively pursued and prosecuted by the federal government using all its capabilities and authorities. Imposing swift and certain consequences upon cyber adversaries, who are often provided safe harbor in non-cooperative foreign jurisdictions, such as Russia, China, Iran and North Korea, is essential to reducing the cyber threats targeting healthcare and the nation.

Cybersecurity and Rural Hospitals

Rural hospitals can face unique risks, challenges and impacts when defending against cyberattacks. Rural hospitals also may face certain infrastructure barriers when it comes to deployment of AI tools. Rural hospitals are geographically remote, often situated in non-metropolitan counties and sometimes well over 100 miles from the nearest hospital. Ransomware attacks, which result in diverting patients and ambulances, can create delays in the provision of critical healthcare services, which can elevate the risk of a negative outcome for the patient.

Rural hospitals also can face financial, human and technical resource challenges, which can affect the ability to respond to the increased cyber threat environment. Most rural hospitals operate on very thin financial margins or negative margins, with 48% of rural hospitals operating at a financial loss in 2023, according to AHA analysis of RAND Hospital Cost Report data. Limited financial resources can impede rural hospitals' ability

to obtain the latest and most advanced cybersecurity technologies to defend and monitor hospital networks 24/7 and to replace aging and insecure third-party technology, such as medical devices. Lack of financial resources also has inhibited rural hospitals' ability to recruit and retain cybersecurity professionals, who are in great demand in higher-paying urban areas, other sectors and government agencies.

We look forward to working with Congress to find solutions to help rural hospitals manage cybersecurity challenges. The AHA supports Chairman Hawley's legislation (S.2169/H.R. 9908) as it would give rural hospitals tools to strengthen cybersecurity and mitigate risks associated with harmful cyber threats by creating a comprehensive workforce strategy to train cybersecurity professionals and develop partnerships to expand the cybersecurity workforce for rural hospitals. We also support workforce grant and retention efforts, with a particular focus on the retraining of veterans.

Conclusion

We stand ready to work with Congress to ensure hospitals and health systems have the resources they need to continue serving their patients and communities. At the same time, we also must enact policies that bolster support for the entire healthcare system's efforts to protect healthcare services, data and patients from cyberattacks.