American Hospital Association™
Advancing Health in America

Washington, D.C. Office
800 10th Street, N.W.
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100

Statement

of the

American Hospital Association

for the

Committee on Health, Education, Labor and Pensions

of the

United States Senate

"Securing the Future of Health Care: Enhancing Cybersecurity and Protecting Americans' Privacy"

July 9, 2025

On behalf of our nearly 5,000 member hospitals and health systems and other health care organizations, our clinician partners — including more than 270,000 affiliated physicians, 2 million nurses and other caregivers the American Hospital Association (AHA) appreciates the opportunity to submit this statement for the record to the Committee on Health, Education, Labor and Pensions hearing, "Securing the Future of Health Care: Enhancing Cybersecurity and Protecting Americans' Privacy."

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 by the loss of personal health care 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 defend against attacks from both criminal and national-state sponsored adversaries. The AHA has also worked with the Health Sector Coordinating Council and the Health-Information Sharing

and Analysis Center (ISAC) to build trusted relationships and channels for the mutual exchange of cyber threat information, develop risk mitigation practices, conduct regional field ransomware attack exercises and share lessons learned from ransomware attacks.

According to U.S. government reporting, the most significant cyber threats targeting U.S. critical infrastructure, including health care, originate from noncooperative foreign jurisdictions.[1,2,3,4] Cross-border hacking incidents, which result in the theft of protected health information (PHI) and ransomware attacks targeting health care have increased dramatically, rising nearly tenfold since 2020. According to the HHS Office of Civil Rights (OCR), the number of individuals impacted by health care data breaches increased from 27 million in 2020 to a staggering 259 million in 2024.[5] It is important to note that most PHI data breaches reported to OCR were the result of hacking incidents targeting non-hospital health care providers, including third-party service and software providers. In 2024, the Change Healthcare ransomware attack alone resulted in the theft of 190 million Americans' PHI — the largest health care data breach in history. The AHA's work in this area was critically important, allowing us to quickly assist members in their response to the Change Healthcare cyberattack. Since 2020, as reported by OCR, 590 million Americans have been impacted by health care breaches, meaning that the entirety of the U.S. population of 330 million individuals has had their health care records compromised in some manner, with most being impacted more than once.

GOVERNMENT'S ROLE IN MITIGATING THE IMPACT OF 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 ongoing and unresolved national security threats. Health care is a top critical infrastructure sector with direct impact on public health and safety, and must be protected. Any cyberattack on the health care 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. Imposing swift and certain consequences upon cyber adversaries, who are often provided safe harbor in noncooperative foreign jurisdictions, is essential to reducing the cyber threats targeting health care and the nation.

CYBERSECURITY CHALLENGES FOR RURAL HOSPITALS

Rural hospitals can face unique risks, challenges and impacts when defending against cyberattacks. Rural hospitals are geographically remote, located in non-metropolitan

---

[1] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf
[2] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
[3] https://usun.usmission.gov/remarks-at-a-un-security-council-briefing-on-ransomware-attacks-against-hospitals-and-other-healthcare-facilities-and-services/
[4] https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors
[5] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

counties, and may be well over a hundred miles from the nearest hospital. Ransomware attacks, which result in diverting patients and ambulances, can create delays in the provision of critical health care services, which can elevate the risk of a negative outcome for the patient.

Rural hospitals can also 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.[6] 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 has also 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. We encourage Congress to provide additional financial resources and support for cybersecurity workforce strategies and training. For example, we support the development of workforce training programs to address the challenges of small and rural facilities. We also support workforce grant and retention efforts, with a particular focus on the retraining of veterans.

CHANGE HEALTHCARE CYBERATTACK

Last year's attack on UnitedHealth Group's Change Healthcare incapacitated significant portions of our health care system's critical functions that keep the health care system operating — from claims processing to clinical information exchange to prescription processing. The attack was the most significant and consequential cyberattack on the U.S. health care system in American history and ultimately exposed data of more than 190 million people. Every hospital in the country felt the impact, either directly or indirectly. Impacts varied depending on factors such as the amount of cash reserves, vendor redundancy and reliance on Change Healthcare technology.

There are several lessons learned from this incident, and AHA would urge Congress to consider the following for future incidents:

- Financial resources, like the Accelerated and Advanced Payments (AAPs) and Temporary Funding Assistance program, and flexibilities in repayment terms were necessary long after systems were restored. Initially, the AAPs were only set up for 30 days and had an aggressive payback schedule. For many hospitals, it took months to fully work through claims backlogs and readjust cash flows. These resources were necessary to keep hospitals afloat while normal operating

[6] AHA analysis of RAND Hospital Cost Report data.

procedures were being restored. In the event of future large-scale incidents, it would be necessary to ensure resources are available for a sufficient time from the date of the incident and that reasonable, gradual repayment schedules are established.

- Given the disruption in operating procedures and systems, HHS guidance was necessary to waive timely filing requirements for claims, extend timelines for appeals, and not deny claims due to lack of authorization/failure to give notice of admission/failure to electronically check eligibility, etc. For future incidents, these waivers and updates to timelines should be enacted sooner, since there is precedent from which to draw.

- With respect to the Change Healthcare incident, the AHA urged for clarification that hospitals and other providers would not be responsible for additional breach notifications if UnitedHealth Group and Change Healthcare were doing so already. Streamlined notification processes would help avoid confusion and misunderstandings with messaging from multiple parties.

- The Change Healthcare incident also underscored the importance of consistent cybersecurity standards across the health care ecosystem. With the rise in PHI data breaches related to third-party vendors, including Change Healthcare, it is imperative that entities not covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) must be subject to the same standards.

DEREGULATION EFFORTS TO SUPPORT DATA PRIVACY AND SECURITY

The AHA supports the administration's goals of reducing barriers for data interoperability and fostering innovation to support better health outcomes. We recognize the pivotal role that health technology plays in care delivery today and its potential to transform the patient and provider experience in the future. Moreover, we believe that technology and data interoperability have the potential to address some of the prevalent challenges confronting the health care ecosystem today, including provider burnout and staffing shortages driven by administrative burdens. We also recognize that the innovative applications of health information technology (IT) must be balanced with reasonable guardrails to protect sensitive patient data and ensure security and privacy.

The AHA highlighted recommendations regarding data security and privacy in response to a request for information from the Centers for Medicare & Medicaid Services and the Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology on the Health Technology Ecosystem.[7] We have also made similar recommendations in response to deregulation requests for information from the

[7] https://www.aha.org/system/files/media/file/2025/06/aha-comments-on-the-cms-and-astp-onc-request-for-information-re-the-health-technology-ecosystem-letter-6-16-2025.pdf

Office of Management and Budget, the Federal Trade Commission and the Department of Justice.[8,9,10] For example, we have urged the agency to modify the HIPAA cybersecurity rule of December 2024 to make the requirements voluntary and to modify the HIPAA Breach Notification Rule to remove the requirement to report breaches affecting fewer than 500 individuals. The AHA does not support proposals for mandatory cybersecurity requirements levied on hospitals as if they were at fault for the success of hackers in perpetrating a crime. Instead, the AHA supports voluntary consensus-based cybersecurity practices such as the cybersecurity performance goals. The now well-documented source of cybersecurity risk in the health care sector, including the Change Healthcare cyberattack, is from vulnerabilities in third-party technology, not hospitals' primary systems. No organization, including federal agencies, is or can be immune to cyberattacks. To make meaningful progress in the war on cybercrime, Congress and the administration should focus on the entire health care sector and not just hospitals.

As part of the AHA's responses to deregulation requests for information, we have also urged the elimination of 42 CFR Part 2 requirements that hinder care team access to important health information and protect patient privacy under HIPAA. Despite regulatory changes in the past several years, the regulations in Part 2 are outdated, fail to protect patient privacy and erect sometimes insurmountable barriers to providing coordinated, whole-person care to people with a history of substance use disorder (SUD). Specifically, the regulations require the separation of records pertaining to SUD information, which prevents the integration of behavioral and physical health care because the patient data cannot be used and disclosed like all other health care data.

HIPAA PREEMPTION

While generally preempting contrary state law, HIPAA does not preempt state law that is "more stringent" than the requirements that it mandates. Specifically, state law is not preempted where: (1) state law is contrary to HIPAA; (2) relates to matters of individually identifiable health information; and (3) is more stringent than the HIPAA requirements.

For all the strengths of the existing HIPAA framework, its approach to preemption has proven to be problematic. It creates unnecessary regulatory burdens on hospitals and health systems, forcing them to satisfy a myriad of legal requirements that raise compliance costs and divert limited resources that could be used on patient care. In addition, the existing state and federal patchwork of health information privacy

---

[8] https://www.aha.org/system/files/media/file/2025/05/aha-response-to-omb-deregulation-rfi-letter-5-12-2025.pdf
[9] https://www.aha.org/system/files/media/file/2025/05/AHA-Comments-on-FTC-Anticompetitive-Deregulations-RFI.pd
[10] https://www.aha.org/system/files/media/file/2025/05/AHA-Comments-on-DOJ-Anticompetitive-Deregulations-RFI.pdf

requirements remains a significant barrier to the robust sharing of patient information necessary for coordinated clinical treatment. For instance, the patchwork of differing requirements poses significant challenges for providers' use of a common electronic health record that is a critical part of the infrastructure necessary for effectively coordinating patient care and maintaining population health.

If Congress were to make any changes to HIPAA, it should address this problem and enact a full preemption provision. HIPAA is more than sufficient to protect patient privacy and, if interpreted correctly, it strikes the appropriate balance between health information privacy and valuable information-sharing. Varying state laws only add costs and create complications for hospitals and health systems. **As such, the AHA reiterates its long-standing recommendation that Congress strengthen HIPAA preemption.**

CONCLUSION

The AHA looks forward to working with Congress to ensure hospitals and health systems have the tools they need to continue to ensure the safety and privacy of their patients and their medical information.