United States Senate

WASHINGTON, DC 20510

July 18, 2025

The Honorable Robert Kennedy, Jr.
Secretary of Health and Human Services
200 Independence Avenue SW
Washington, DC 20201

The Honorable Mehmet Oz
Administrator
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, MD 21244

Dear Secretary Kennedy and Administrator Oz,

We write to express our alarm at the negative impacts of Trumpcare on the cybersecurity resiliency of rural hospitals and to request clear information about your plans to address these harms.

On Friday, July 4, 2025, President Donald Trump signed into law the largest cuts to the United States health care system in American history. According to the nonpartisan, independent Congressional Budget Office (CBO), this rushed, reckless bill will cut over $1 trillion from the U.S. health care system.[1] Trump's health care cuts will cause 17 million Americans to lose their health insurance coverage and put additional strain on hundreds of hospitals across the country. Rural and small hospitals will face disproportionate impacts. Over 330 rural hospitals that are already financially vulnerable will be forced into making impossible choices in order to stay open, continue to serve the health care needs of patients, and employ large swaths of rural communities.[2]

Republicans in Congress rushed their bill through with virtually no transparency, no external vetting, and minimal analyses or input from affected health care providers. While CBO quantified the devastating impacts of this bill on Americans' access to affordable health care, there are many downstream, devastating consequences yet to be uncovered. One potential impact

[1] Congressional Budget Office (CBO). (2025, June 27). *Estimated Budgetary Effects of an Amendment in the Nature of a Substitute to H.R. 1, the One Big Beautiful Bill Act, Relative to the Budget Enforcement Baseline for Consideration in the Senate.* Congressional Budget Office. https://www.cbo.gov/publication/61533

[2] United States Senator Markey. (2025, June 12). *Markey, Leader, Schumer, Wyden, Merkley Release Data Detailing Hundreds of Rural Hospitals Across U.S. at Risk Due to Republican Health Care Cuts.* https://www.markey.senate.gov/news/press-releases/markey-leader-schumer-wyden-merkley-release-data-detailing-hundreds-of-rural-hospitals-across-us-at-risk-due-to-republican-health-care-cuts a

of these extensive health care cuts is degrading cyber resiliency, which may increase cyberattacks that will shut down the ability of hospitals to provide patients with lifesaving care.

According to the HHS Administration for Strategic Preparedness & Response, health care facilities are a prime target for cyber criminals because of "their size, technological dependence, sensitive data, and unique vulnerability to disruptions."[3] Bad actors know that health care facilities, particularly hospitals, have troves of valuable patient data and weak infrastructure to protect this medical information from theft. Fraudsters can use this sensitive patient data for fraudulent billing practices, like buying and selling expensive medical devices, or even to blackmail patients. Hospitals are also very likely to pay a ransom in order to protect patient data and continue with daily operations as quickly as possible.[4]

Rural hospitals and small hospitals already struggle to find the necessary funds to invest in cybersecurity defenses to protect patient information or computer systems and other infrastructure used to deliver health care. These facilities have to weigh challenging tradeoffs when considering the resources needed to upgrade and maintain their cybersecurity infrastructure, replace their aging information technology systems, and train their staff with comprehensive cybersecurity training.[5] Rural and small hospitals are less likely to have dedicated staff to respond to cybersecurity vulnerabilities and breaches, and they are more likely to outsource these critical functions.[6] And hackers know that rural and small hospitals are highly motivated to maintain the continuity of health care given the lack of nearby providers, especially emergency services and procedures, and their top priority is protecting the health and well-being of patients they serve.

As rural and small hospitals confront even lower operating margins due to Republican health care cuts, they will be less likely to prioritize spending on cybersecurity infrastructure. The financial impact of ransomware attacks has already led one rural hospital to close.[7] In addition, rural hospitals and small hospitals are already foregoing planned cybersecurity investments as

[3] Assistant Secretary for Preparedness & Response. *Healthcare Sector Cybersecurity.* HHS. https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf

[4] National Rural Health Association. (2025, April 17). *Rural hospital cybersecurity is a critical health issue.* NRHA. https://www.ruralhealth.us/blogs/2025/04/rural-hospital-cybersecurity-is-a-critical-health-issue

[5] National Rural Health Association. (2025, April 17). *Rural hospital cybersecurity is a critical health issue.* NRHA. https://www.ruralhealth.us/blogs/2025/04/rural-hospital-cybersecurity-is-a-critical-health-issue

[6] U.S. Department of Health and Human Services. (2023, April). Hospital Cyber Resiliency Initiative Landscape Analysis. HHS 405(d). https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf

[7] Schwartz, N. (2023, June 15). *Rural hospital cybersecurity protection bill moves forward.* Becker's Health IT. https://www.beckershospitalreview.com/healthcare-information-technology/cybersecurity/ransomware-attack-causes-illinois-hospital-to-close/

they anticipate Republicans' health care cuts.[8] This will lead to devastating impacts in rural communities and the entire health care system and puts patient care and safety at increased risk.[9]

Trumpcare will harm the cybersecurity resiliency of rural and small hospitals just as this Administration has chosen to gut cybersecurity operations at HHS. In March, HHS announced a formal plan to reorganize the agency and centralize IT functions, reducing the staff who were responsible for protecting sensitive patient data from cybersecurity breaches by contractors and other third parties.[10] In addition, the HHS Office of Civil Rights (OCR), which is charged with investigating hacks and protecting privacy, has shifted its limited resources away from investigating cybersecurity breaches, further undermining its minimal oversight functions.[11] The lack of federal oversight and resources, coupled with historic cuts to Medicaid and the Affordable Care Act (ACA), only serve to increase rural and small hospitals' cybersecurity vulnerabilities.

It is critical that HHS do everything in its power to protect rural hospitals from cyber attacks. Given the urgency of this situation, we ask you to answer the following questions in writing by Friday, July 25:

1. What plans do HHS and CMS have in place to make sure that rural hospitals and small hospitals implement HHS' Healthcare and Public Health (HPH) essential and enhanced Cybersecurity Performance Goals?[12]

    a. Under what timeframe does HHS expect all rural and small hospitals comply with the voluntary essential cybersecurity performance goals? Under what timeframe does HHS expect all rural and small hospitals to meet the voluntary enhanced cybersecurity performance goals?

[8] Nickel, D. & Miller, M. (2025, July 7). *Hospital cybersecurity is a potential megabill casualty.* Politico. https://www.politico.com/newsletters/weekly-cybersecurity/2025/07/07/hospital-cybersecurity-is-a-potential-megabill-casualty-00441066

[9] https://www.statnews.com/2023/11/17/hospital-ransomware-attack-patient-deaths-study/

[10] U.S. Department of Health and Human Services. (2025, March 27). *Fact Sheet: HHS' Transformation to Make America Healthy Again.* HHS. *https://www.hhs.gov/press-room/hhs-restructuring-doge-fact-sheet.html#:~:text=The%20current%2082%2C000%20full%2Dtime,and%20Policy%20will%20be%20centralized*, Gilbert, D. (2025, April 14). *HHS Systems are in Danger of Collapsing, Workers Say.* Wired. https://www.wired.com/story/department-health-human-services-possible-collapse/

[11] Cirruzzo, C., Hooper, K., & King, R. (2025, April 30). *HHS switches gears: Cybersecurity out, DEI bans in.* Politico Pulse. https://www.politico.com/newsletters/politico-pulse/2025/04/30/hhs-switches-gears-cybersecurity-out-dei-bans-in-00316786

[12] U.S. Department of Health and Human Services. *HPH Cybersecurity Performance Goals.* https://hhscyber.hhs.gov/performance-goals.html

b. What resources, including grant funding or other financial assistance and technical assistance, are HHS and CMS providing to rural and small hospitals to meet these cybersecurity performance goals?

c. Are HHS and CMS working with third party vendors to provide financial support or technical assistance to rural and small hospitals as they seek to meet cybersecurity performance goals? If so, which third parties are HHS and CMS working with?

d. If HHS and CMS do not have plans to make sure rural and small hospitals achieve the HPH Cybersecurity Performance Goals, then which standards will HHS and CMS make sure rural hospitals adhere to in order to improve their cybersecurity resiliency and how has HHS determined that these alternate standards are effective defending against hacks? Please provide written details of the cybersecurity standards that rural hospitals will be expected to meet.

2. The Republican reconciliation bill provided $50 billion for a new so-called "Rural Health Transformation Program." This vague, paltry fund gives the CMS Administrator broad discretion to award states that pledge to, "...prioritize data and technology driven solutions that help rural hospitals." States will be allowed to use funds they receive to develop "technology-enabled solutions that improve care delivery in rural hospitals" and to provide "significant information technology advances designed to improve efficiency, enhance cybersecurity capability development, and improve patient health outcomes."

   a. What specific protocols will HHS and CMS use to evaluate a state's plan to use funding from the Rural Health Transformation Program for "technology-enabled solutions" and "significant information technology advances"?

   b. What process will HHS and CMS use to make sure that funding from the Rural Health Transformation Program spent on technology-enabled solutions and information technology advances does not expose states or rural hospitals to cybersecurity vulnerabilities? Will HHS and CMS develop a protocol to make sure that any third-party vendors that receive federal funds are meeting specific cybersecurity standards? If so, please provide this protocol in writing.

   c. Has HHS and/or CMS already promised or guaranteed funding from the Rural Health Transformation Program to certain states, companies, or vendors who can provide these technology-based solutions and information technology advances? If so, to which states, companies, or vendors have you guaranteed this funding?

3. The Republican reconciliation bill also provided $200 million in implementation funding to CMS to establish the new $50 billion Rural Health Transformation Program.

   a. How do HHS and CMS intend to use this implementation funding?

   b. Do HHS and CMS plan to use implementation funding to hire a third-party vendor to award funds to states?

   c. If HHS and CMS plan to hire a third-party vendor to award funds to states, then what protocols will the agencies use to make sure that these vendors adhere to specific cybersecurity standards?

4. Have you implemented plans to restructure information technology functions at HHS as outlined in your March announcement?

   a. If so, have all information technology functions at HHS been centralized?

   b. How many full-time equivalents (FTEs) currently oversee the protection of sensitive patient health information?

5. Does OCR continue to investigate cybersecurity breaches at health care facilities, including rural hospitals and small hospitals?

   a. It is my/our understanding that OCR has lacked sufficient funding to investigate cybersecurity breaches at health care facilities. Does OCR now have sufficient funding to carry out these functions? If so, then how has the funding for OCR to complete these functions changed over the past year?

   b. If not, which operating division within HHS is responsible for these investigations?

   c. Please provide a breakdown of how much federal funding and how many FTEs at HHS are dedicated to cybersecurity breach investigations.

6. In January, 2025, HHS issued a proposed rule to update and modify the Health Insurance Portability and Accountability Act of 1996 (HIPAA) rules to strengthen cybersecurity protections for electronic protected health information. These requirements have not been meaningfully updated since 2003. What is the status of the proposed rule? Does HHS intend to finalize this rule?

It is clear that you were motivated to quickly pass Trumpcare and made many public and private appeals to lawmakers to get this bill enacted. Members of Congress and the public deserve full transparency about these commitments and HHS' plans to address the additional cybersecurity vulnerabilities that will be thrust on rural and small hospitals across the country because of the bill's catastrophic cuts.

We therefore expect you to share a detailed plan and written responses to the above questions outlining the guarantees you made to lawmakers about how you intend to minimize the negative impacts of this bill on rural hospitals, including any heightened risks that will result from spending cuts that will compromise hospitals' implementation of effective cybersecurity practices. We look forward to your thorough and timely response.

Sincerely,

Ron Wyden

Ron Wyden
United States Senator
Ranking Member, Committee
on Finance

Mark R Warner

Mark R. Warner
United States Senator