



Hacking Healthcare- Weekly Blog

Hacking Healthcare

TLP:WHITE

Alert ID : 7a70617c

Jul 17, 2025, 11:49 AM



This week, Health-ISAC®'s Hacking Healthcare® examines rural healthcare cybersecurity priorities of the U.S. legislative branch. Join us as we identify the Congressional members who are leading cybersecurity efforts, current legislation that could have an effect on health sector cybersecurity, cybersecurity areas that may see legislative attention in the near future, and how the ongoing appropriations process for fiscal year 2026 (FY26) could affect relevant U.S. government departments and agencies.

Welcome back to Hacking Healthcare®.

U.S. Rural Healthcare Cybersecurity Priorities in Congress

Congressional attention for the past many weeks was heavily focused on getting H.R.1, the One Big Beautiful Bill Act, to President Trump's desk. With that now accomplished, there is a bit more capacity to address other matters, including a range of cybersecurity and technology issues that may affect the health sector. But what are these issues, who is supporting them, and what might we learn from the ongoing appropriations process?[i]

The State of Rural Hospital Cybersecurity

Alarm has been continuously raised about the plight of rural healthcare in the U.S. over the past few years. Specifically, the high and ever-increasing number of hospital and clinic closures. Some sobering statistics include:

1. A reported 197 Rural Hospital Closures and Conversions between January 2005 and October 2023.[\[ii\]](#)
2. A reported risk of nearly 700 rural hospitals at risk of closing.[\[iii\]](#)
3. A reported 48% of rural hospitals operated at a financial loss in 2023.[\[iv\]](#)

There are a variety of reported reasons for the state of rural healthcare, from what private insurers are willing to pay for healthcare services to inefficiencies and inadequacies of Medicare and Medicaid.[\[v\]](#), [\[vi\]](#) It is also expected that provisions within H.R.1 that cut Medicaid spending will amplify these concerns, as evidenced by Sen. Hawley's attempt to mitigate the effects of those provisions through a new bill, despite recently voting for H.R. 1. [\[vii\]](#), [\[viii\]](#), [\[ix\]](#), [\[x\]](#)

While the root causes of rural hospital and clinic struggles, and the policy approaches to address them, are out of scope of this article, the ramifications for healthcare cybersecurity are fairly straightforward. Health sector entities that operate at a financial loss, or near loss, are likely to struggle to acquire and maintain staff and modern IT/OT infrastructure. Furthermore, cybersecurity is likely to be deprioritized only to what is necessary to remain compliant with laws and regulations. General cybersecurity workforce shortages further exacerbate this issue, a problem felt acutely by rural areas that often struggle to bring in and retain cybersecurity and technical talent.

Congress has put forward a few legislative bills to help address the problems above, these include:

1. S.2169 — Rural Hospital Cybersecurity Enhancement Act — Introduced by Sen. Hawley [R-MO] at the end of June, and co-sponsored by three Democrats, the bill seeks to require the Secretary of Health and Human Services to develop a "comprehensive rural hospital cybersecurity workforce development strategy to address the growing need for skilled cybersecurity professionals in rural hospitals."[\[xi\]](#) It also seeks to create "instructional materials for rural hospitals that can be used to train staff on fundamental cybersecurity efforts."[\[xii\]](#)

1. H.R.3063 — Rural Hospital Stabilization Act of 2025 — Introduced by Rep. Shomari [D-AL-2] at the end of April, and co-sponsored by eight Democrats and Republicans, the bill seeks to "amend the Public Health Service Act to authorize the Secretary of Health and Human Services to make grants to assist rural hospitals." Grants would be eligible for "projects to acquire, repair, and upgrade the systems, facilities, and

equipment of rural hospitals," and for providing "financial assistance to be used toward the operational costs of rural hospitals, including payroll expenses."^[xiii]

Congress has also hinted at potentially introducing more legislation to help address the problems above. At the recent Senate Committee on Health, Education, Labor & Pensions hearing, "Securing the Future of Health Care: Enhancing Cybersecurity and Protecting Americans' Privacy," Senator Cassidy [R-LA] noted his desire to do the following:

1. Reintroduce his Health Care Cybersecurity and Resiliency Act — Introduced in the last senate and co-sponsored by two Democrats, the bill sought to "require the Secretary of Health and Human Services and the Director of the Cybersecurity and Infrastructure Security Agency to coordinate to improve cybersecurity in the health care and public health sectors."^[xiv] Among its many provisions, it would update the current breach reporting portal and breach reporting obligations, introduce required baseline cybersecurity standards, require the creation of guidance to rural entities on best practices to improve cyber readiness, amend the Public Health Service Act to facilitate grants to enhance cybersecurity, and address workforce concerns with training and a strategy.

1. Find ways to support rural healthcare providers' utilization of AI.

Notably, the issue has also been raised with soon-to-be senior members of the Trump Administration.

1. During the Senate Committee on Homeland Security and Governmental Affairs nomination hearing on June 5 that included National Cyber Director nominee Sean Cairncross, Sen. Hawley highlighted the pressing cybersecurity issues facing rural healthcare entities and received assurances from Cairncross that he was very interested in working on the issue.^[xv]

Action & Analysis

Included with Health-ISAC Membership

[i] Please note that the scope of Hacking Healthcare does not allow us to cover all congressional issue areas that may have an effect on health sector cybersecurity.

[ii] <https://www.shepscenter.unc.edu/programs-projects/rural-health/rural-hospital-closures/>

[iii] <https://ruralhospitals.chqpr.org/>

[iv] <https://www.aha.org/fact-sheets/2025-06-13-rural-hospitals-risk-cuts-medicaid-would-further-threaten-access#fn2>

[v] <https://time.com/7298891/rural-hospitals-closing-explained-health-care/>

- [vi] <https://ruralhospitals.chqpr.org/Problems.html#the-magnitude-of-financial-losses-at-rural-hospitals>
- [vii] <https://www.aha.org/fact-sheets/2025-06-13-rural-hospitals-risk-cuts-medicaid-would-further-threaten-access#fn2>
- [viii] <https://time.com/7298891/rural-hospitals-closing-explained-health-care/>
- [ix] <https://abcnews.go.com/US/wireStory/rural-hospitals-brace-financial-hits-closure-republicans-1-123474194>
- [x] <https://thehill.com/policy/healthcare/5402636-hawley-seeks-to-repeal-medicaid-cuts-he-voted-for/>
- [xi] <https://www.congress.gov/bill/119th-congress/senate-bill/2169/text>
- [xii] <https://www.congress.gov/bill/119th-congress/senate-bill/2169/text>
- [xiii] <https://www.congress.gov/bill/119th-congress/house-bill/3063/text>
- [xiv] <https://www.congress.gov/bill/118th-congress/senate-bill/5390/text>
- [xv] <https://www.hsgac.senate.gov/hearings/nominations-10/>
- [xvi] <https://www.whitehouse.gov/omb/information-resources/budget/the-presidents-fy-2026-discretionary-budget-request/>
- [xvii] <https://health-isac.cyware.com/webapp/user/myfeeds/49c15eee>
- [xviii] <https://health-isac.cyware.com/webapp/user/myfeeds/ea84732f>
- [xix] <https://health-isac.cyware.com/webapp/user/myfeeds/8a256f94>

Report Source(s)

Health-ISAC

Release Date

Jul 17, 2025, 12:00 AM

Reference

- cyware
- senate
- chqpr
- go
- cyware
- time
- congress
- thehill
- whitehouse
- cyware
- congress
- aha
- unc
- congress
- chqpr

[chqpr](#)

Tags

Rural, Hacking Healthcare, Congress

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Conferences, Webinars, and Summits:

<https://h-isac.org/events/>

Hacking Healthcare:

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Councils efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Councils Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISACs annual Hobby Exercise and provides legal and regulatory updates for the Health-ISACs monthly Threat Briefing.

1. John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
2. Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Threat Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments:

Please email us at toc@h-isac.org