National Rural Health Association

https://www.ruralhealth.us/advocate
@nrha_advocacy

Rural Cybersecurity

Studies have shown that small healthcare providers with under 500 employees suffer disproportionately compared to the broader healthcare sector.

Security breaches **increased 84%** from 2018 to 2021, with **66% of health care organizations** say they experienced some type of cyberattack.

84%

of ransomware attacks on rural hospitals resulted in significant operational disruptions including:

- Electronic system downtime (81%)
- Delays or cancellations in scheduled care (42%)
- Ambulance diversion (33%)

Reported average number of days in downtime following an attack is:

18.7 days

Cybersecurity attacks disruptions are **more detrimental in rural areas** given the greater distances patients must travel to receive care and the outsized impact that lost revenue may have on rural hospital finances.

Rural Cybersecurity Support Resources

Microsoft Cybersecurity Program for Rural Hospitals

A collaboration between Microsoft and the National Rural Health Association, among others, offers rural hospitals access to Microsoft security solutions, resources, and training at no cost.

Google Rural Healthcare Cybersecurity Initiative

Aims to help rural health systems and hospitals strengthen their resilience to cyberattacks. Google is partnering with NRHA and other government and industry partners to offer its solutions to rural health facilities at no cost or a significant discount.

NRHA Legislative Proposals

S. 2169: Rural Hospital Cybersecurity Enhancement Act

Sens. Hawley (R-MO), Hassan (D-NH), Kelly (D-AZ)

Requires the Cybersecurity and Infrastructure Security Agency (CISA) to develop and annually report to Congress about a workforce development strategy to address the unmet need for cybersecurity professionals in rural hospitals. Additionally, CISA must disseminate materials that rural hospitals may use to train staff about cybersecurity.