National Rural Health Association Policy Brief

# Cybersecurity: A path to increase rural health care preparedness

*Authors: Michael Hassell, Jenny Niblock*

## Introduction

Rural health care organizations are in urgent need of increased cybersecurity measures to address the growing threats and vulnerabilities present with the increase of digital patient records. Rural health facilities face insufficient funding, infrastructure, resources, and personnel to successfully achieve the level of cybersecurity needed to protect patient information.

Rural health care organizations play a critical role in providing access to medical services for remote and frontier populations. Health care delivery is increasingly a digital experience. The need for robust and up-to-date cybersecurity is paramount. A patient's sensitive health information is now entirely handled in an electronic medical record that is readily distributed, shared, and accessible. Cyber preparedness to prevent and respond to attacks is more important than ever.

Cyberattacks are not new to health care, but over the last decade, security breaches have become more common in rural areas. Cyber thieves are targeting rural organizations more frequently as larger urban centers are more prepared to prevent attacks. Estimates indicate that a patient's medical record is worth 10 times more on the black market than a credit card number.[3] Hackers target data including personal identification information such as social security numbers and birthdate, protected patient records, and financial information such as credit card and bank account details. Stolen medical records are used to buy medical equipment and drugs for resale or to file fraudulent insurance claims. Unlike credit card fraud, health care deception often can go on for years before it is discovered by patients who do not often look at their health care records or detailed bill. The estimated cost of remediating a health care record breach is $418 per person. Losing access to hijacked medical records can jeopardize the care of patients and become a regional disaster for the rural hospital's service area.[1]

Proper preparedness to protect patients' sensitive records is estimated to prevent 80 percent of cyberattacks. However, the confusing and sometimes competing patchwork of rules and guidance from federal and state agencies is a major reason why the industry has struggled to mount more effective defenses.[6] Rural health care facilities frequently lack the funding and expertise to be adequately prepared to enact and maintain strong cybersecurity practices and policies due to low-to-negative operating margins. Limited resources to maintain and upgrade cybersecurity infrastructure also serves as a barrier. Due to limited resources, rural health care staff may not receive comprehensive cybersecurity training, leaving them unaware of potential threats and the best practices to mitigate them. This knowledge gap increases the vulnerability of their digital systems and data.

## Analysis

Over the last few years, health care facilities have experienced a dramatic increase in the number of cyberattacks and the cost associated with recovery. Approximately 66 percent of health care organizations say they experienced some type of cyberattack in 2021, and security breaches increased 84 percent from 2018 to 2021.[5] Cyberattacks currently impact more than 88 million patients annually, up 60 percent from last year.[2] Recent rural hospital closures can be attributed to the financial impact of cyberattacks.[4] Rural health clinics are one of the top targets for cyberattacks.[5] Experts recommend that rural health care facilities establish short-term strategies to handle ransom payment and downtime operations, while also implementing long-term strategies such as investing in more robust cybersecurity.[2]

## Policy recommendations

- *Increase funding and resources:* Federal and state governments should allocate additional funding and resources to enhance cybersecurity in rural health care settings. This could include grants, subsidies, or tax incentives to facilitate the adoption of cybersecurity technologies, update outdated equipment that does not meet cybersecurity requirements, and training programs to prevent and recognize cyberattacks.
- *Establish regional cybersecurity support centers:* State and local governments, in collaboration with health care associations and technology providers, should establish regional cybersecurity support centers. These centers would provide specialized assistance, training, and guidance on cybersecurity best practices to rural health care organizations.
- *Enhance internet connectivity:* Governments and telecommunication companies should prioritize improving broadband connectivity in rural areas. This would enable rural health care organizations to access cloud-based security solutions, receive real-time threat intelligence, and facilitate secure data exchange.
- *Strengthen cybersecurity education and training*: Governments, in partnership with academic institutions and professional organizations, should develop targeted cybersecurity education and training programs for rural health care professionals. This would enhance their awareness of cybersecurity risks, preventive measures, incident response, and data privacy.
- *Foster collaboration and information sharing*: Encourage collaboration between rural health care organizations, government agencies, and cybersecurity experts to foster information sharing and the exchange of best practices. This could be facilitated through regional or national health care cybersecurity forums, workshops, and online platforms.

## Recommended actions

- Encourage the Department of Homeland Security and Cybersecurity Infrastructure and Security Agency to develop consistent standardized cybersecurity practices and roadmaps, reporting, and auditing tailored to rural health care, aligning current guidance from the U.S. Departments of Health and Human Services, Homeland Security, Justice, Education, Treasury, and Commerce.
- Create state offices or enhance current programs such as Flex to assist rural health care entities with technical assistance, cybersecurity training, staff augmentation, and breach support.
- Support IT workforce development and training with an emphasis on health IT to improve rural entities' ability to attract and retain staff. Encourage partnerships with rural community colleges and technical schools.
- Update and strengthen dated HIPAA rules and regulations to align with the increased use of technology in the health care sector.
- Support S.1560, Rural Hospital Cybersecurity Enhancement Act, to develop a comprehensive work plan to address the staff needs of rural facilities within a year of enactment. A partnership will be developed between rural facilities, the private sector, educational institutions, and nonprofits to increase cybersecurity education and teaching.

## Conclusion

Rural health clinics, hospitals, and health care entities lack funding, personnel, and preparedness to prevent and respond to cyberattacks. Addressing these challenges and implementing increased cybersecurity measures in rural health care facilities is crucial to protect patient data, ensure the continuity of care, and maintain public trust in the health care system. By investing in robust security infrastructure, promoting cybersecurity awareness and training, and adopting best practices, rural health care providers can significantly mitigate the risks posed by cyber threats and safeguard their critical systems and sensitive patient information.

Enhancing cybersecurity in rural health care settings requires a collaborative effort involving governments, health care organizations, technology providers, and cybersecurity experts. By allocating resources, improving infrastructure, providing education and training, fostering collaboration, and implementing appropriate regulations, policymakers can significantly reduce cybersecurity risks and protect the integrity of patient data in rural health care settings.

## References


1. Mclaughlin J. Cyberattacks on Hospitals "Should Be Considered a Regional Disaster. npr.org. Published June 2023. Accessed September 13, 23AD. www.npr.org/2023/06/25/1184025963/cyberattacks-hospitals-ransomware
2. Neprash et al. NH. Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations. *JAMA Health Forum*. 3(129):12,29.
3. Riggi J. The Importance of Cybersecurity in Protecting Patient Safety | Cybersecurity | Center | AHA. aha.org. Published 2022. Accessed September 13, 2023. www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety
4. Schwartz N, ed. *Rural Hospital Cybersecurity Protection Bill Moves Forward*. Beckers Hospital Review; 2023.
5. Stringfellow A. Healthcare and Cybersecurity: 35 Key Statistics and Facts You Should Know. tausight.com. Published November 1, 2022. Accessed September 13, 2023. www.tausight.com/healthcare-and-cybersecurity-key-statistics/
6. Yeo, LH; Banfield, James, ed. *Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis*. Vol 19. National Institutes of Health; 2022.