POLICY BRIEF
June 2024

UNIVERSITY OF MINNESOTA
RURAL HEALTH
RESEARCH CENTER

Understanding the Rise of Ransomware Attacks on Rural Hospitals

Hannah T. Neprash, PhD
Claire C. McGlave, MPH
Katie Rydberg, MPH
Carrie Henning-Smith, PhD, MPH, MSW

Key Findings

- Rural hospitals experienced an increasing number of ransomware attacks from 2016 to 2021.
- From 2016-2021, 43 rural hospitals across 22 states experienced a ransomware attack.
- Ransomware attacks afflicted all types of rural hospitals, including Critical Access Hospitals (N=9), Sole Community Hospitals (N=13), Rural Referral Centers (N=3), and hospitals paid under Medicare's Inpatient Prospective Payment System (N=18).
- 84% of ransomware attacks on rural hospitals resulted in operational disruptions. Common disruptions included electronic system downtime (81%), delays or cancellations in scheduled care (42%), and ambulance diversion (33%). Operational disruptions were similar in rural and urban hospital settings.

rhrc.umn.edu

Purpose

Hospitals face a growing threat from ransomware attacks that are designed to disrupt care delivery and may consequently threaten patient outcomes and hospital finances. While this overall phenomenon has received media and research attention, little is known about ransomware attacks on hospitals in rural areas. This policy brief presents findings from a novel database of hospital ransomware attacks, focusing on the frequency and characteristics of ransomware attacks on rural hospitals.

Background and Policy Context

As hospitals have increased their reliance on health informa-tion technology, they have also increased their susceptibility to new cybersecurity risks, such as ransomware attacks. Ransom-ware is a type of malicious software that blocks users from access-ing their electronic systems and demands a ransom (i.e., finan-cial payment) to restore access.[1,2] To motivate prompt payment of ransom demands, these cyberattacks are designed to disrupt business operations. In the context of hospital operations, ran-somware attacks can disrupt care delivery in many ways – such as by disabling electronic health records and forcing clinicians to chart using pen and paper; by rendering imaging, lab, and electronic monitoring equipment unusable; by forcing hospitals to delay or cancel scheduled surgeries; and even necessitating the use of ambulance diversion protocols (i.e., when a hospital requests that emergency medical services transport patients to alternative facilities). These care disruptions have the potential to threaten patient safety and health outcomes, in addition to hospital finances.

In a rural setting, hospital ransomware attacks may be partic-ularly harmful. First, rural hospitals may be more susceptible to cybersecurity threats like ransomware attacks, due to under-re-sourced information technology (IT) infrastructure and staff.[3-5] Second, the financial consequences of a ransomware attack may be especially dire for rural hospitals, given the already precarious financial circumstances that many face.[6,7] Lost revenue during a ransomware attack was cited as a major reason in the closure of St. Margaret's Health, a rural hospital located in Bureau Coun-ty, Illinois.[8] Third, care disruptions may affect patient outcomes more, if the next-closest health care facility is many miles away, rather than down the street. For example, patients experiencing acute cardiovascular emergencies (i.e., heart attack, stroke, and sepsis) require prompt treatment in order to maximize their survival probabilities.[9-11] During a ransomware attack on a rural hospital, treatment delays for those patients may be the difference between life and death.

Despite these potential harms, there exists little systematic research on the rise of ransomware attacks on rural hospitals. Existing work documents the overall increase in ransomware activity among health care providers, without focusing on geography.[12] One study finds that ransomware-attacked hospitals are somewhat less likely to be located in rural than urban areas,[13] but rural hospitals are not immune from the overall trend. Furthermore, they may experience disproportionately harmful effects when they are attacked, due to their limited ability to divert patients or call-in additional staffing resources. In this policy brief, we characterize the growth in ransomware attacks on hospitals, by rural versus urban locations. As policymakers increasingly focus on improving the cybersecurity preparedness of rural hospitals,[14,15] it is important to disaggregate overall trends by geographic location in order to design tailored and effective policy interventions.

Approach

To assess trends in ransomware attacks on rural hospitals, we used the Tracking Healthcare Ransomware Events and Traits (THREAT) database. This data resource (created by members of this study team) documents ransomware attacks on health care providers, occurring from 2016 to 2021. Described in greater detail elsewhere,[12] the THREAT data combines proprietary data provided by HackNotice (a cybersecurity threat intelligence company that helps businesses identify and respond to attacks) with data from the US Department of Health and Human Services (HHS) Office of Civil Rights Data Breach Portal. The latter includes publicly available information that is collected when Health Insurance Portability and Accountability Act–covered entities report breaches of protected health information, as mandated by the Health Information Technology for Economic and Clinical Health Act of 2009. Beyond these data sources, the THREAT database also includes information collected via supplemental sources – including press releases, public disclosure-of-data-breach letters, local news reports, and health care trade press coverage. For each of the 374 ransomware attacks recorded in the THREAT database, we observe the type of facility affected (i.e., hospital, clinic, etc…), a list of hospitals involved and their geographic locations, date of ransomware attack discovery, whether any operational disruption resulted from the ransomware attack, and the type of operational disruption (i.e., electronic system downtime, cancelled or delayed care, and/or ambulance diversion).

Using the THREAT database, we identified 160 hospitals that experienced a ransomware attack between 2016 and 2021 and then incorporated characteristics of those hospitals from the American Hospital Association Annual Survey data. Using hospital ZIP code, we classified each ransomware-attacked hospital as urban or rural based on the Federal Office of Rural Health Policy methodology, which uses Office of Management and Budget definitions of rural (non-metropolitan) and urban (metropolitan).[16,17] We additionally identified hospital type (i.e., Critical Access Hospital, Sole Community Hospital, Rural Referral Center, or Medicare Inpatient Prospective Payment System hospital).

We mapped the geographic location (using ZIP code) for each ransomware-attacked hospital, distinguishing urban and rural hospitals visually. We also calculated descriptive statistics, including the annual count of ransomware-attacked hospitals in rural versus urban areas, the count of rural ransomware-attacked hospitals by hospital type, and the share of rural versus urban hospitals experiencing different types of operational disruptions during ransomware attacks.

Results

Our sample consisted of 160 hospitals that experienced ransomware attacks between January 1, 2016 and December 31, 2021. Of these, 43 hospitals (26.9%) were rurally located. Figure 1 displays the number of hospitals experiencing ransomware attacks annually, by rural versus urban location. The number of rural ransomware-attacked hospitals increased from 5 in 2016 to 17 in 2021. Figure 2 plots the geographic location of hospitals that experienced ransomware attacks from 2016 to 2021. During this time period, 32 states contained at least one ransomware-attacked hospital, 22 of which contained at least one ransomware-attacked rural hospital.

Figure 3 presents the number of rural hospitals experiencing ransomware attacks, by hospital type. Of the 43 rural hospitals that experienced a ransomware attack, 18 were paid under Medicare's Inpatient Prospective Payment System, 13 were classified as Sole Community Hospitals, 9 were classified as Critical Access Hospitals, and 3 were classified as rurally-located Rural Referral Centers.

Figure 1. Annual Count of Hospital Ransomware Attacks, by Rurality

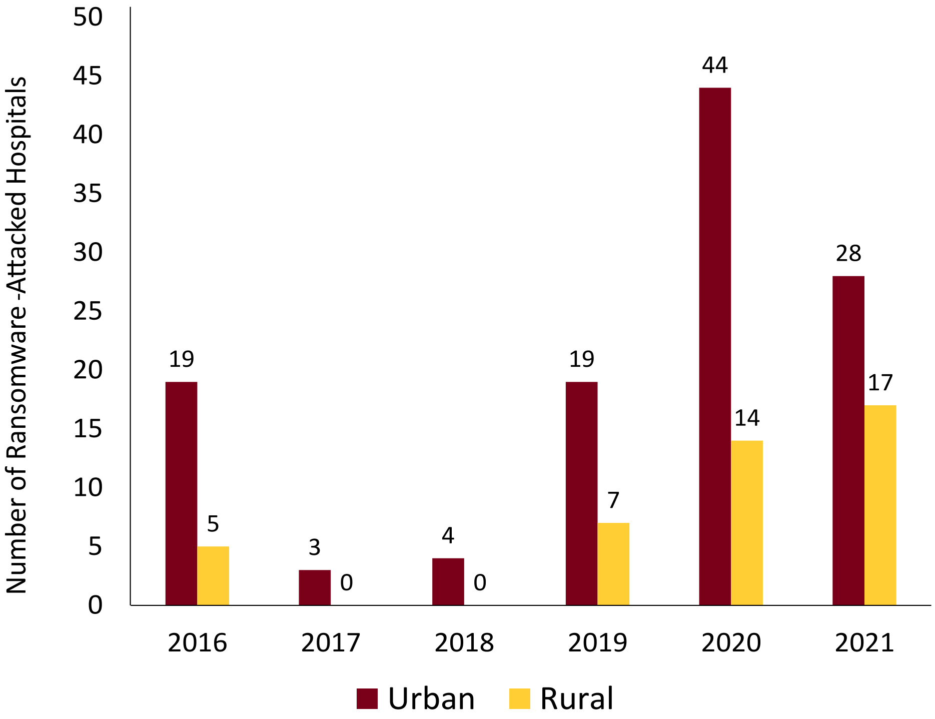


Figure 2. Map of Hospital Ransomware Attacks, by Rurality

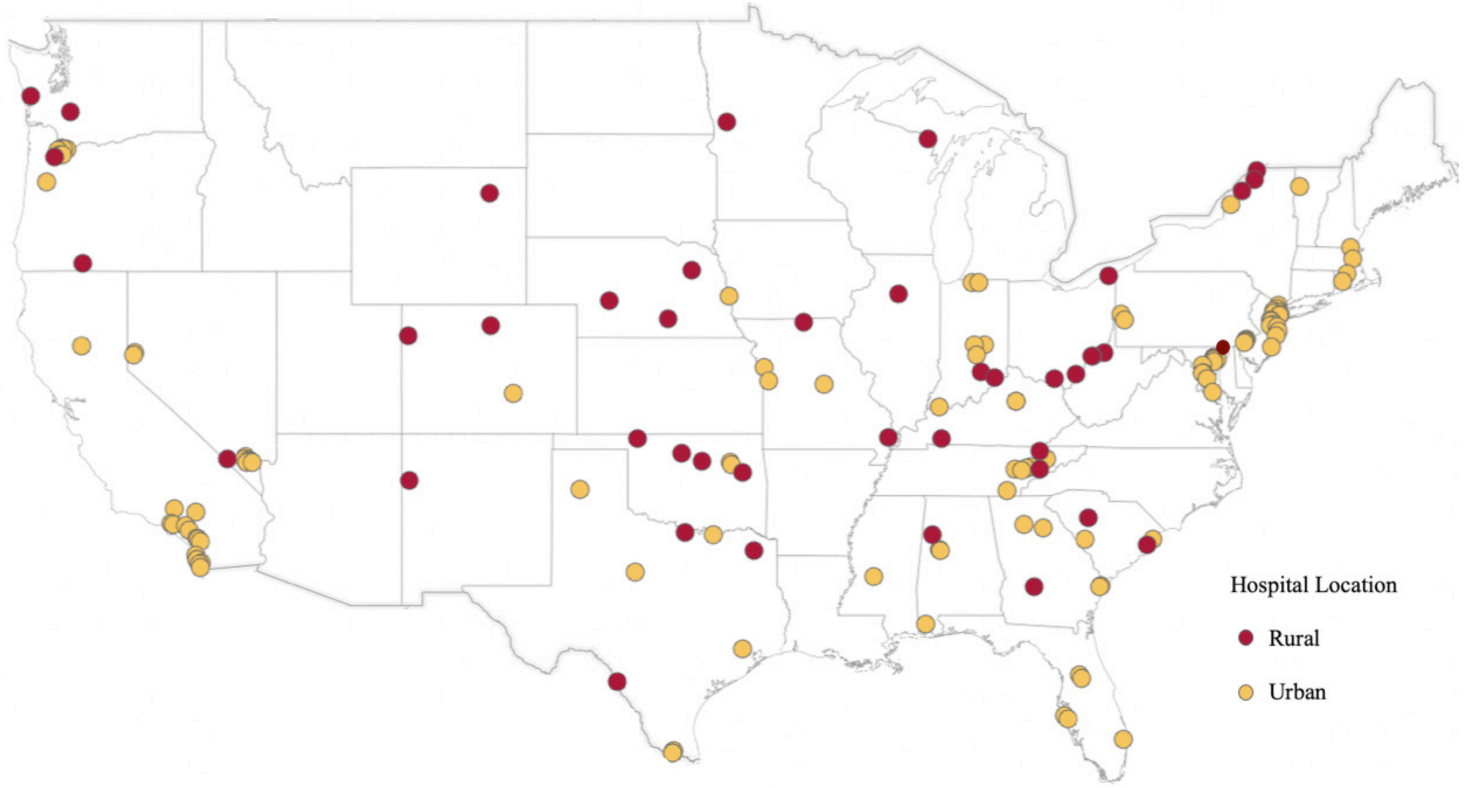


Figure 3. Types of Rural Hospitals Experiencing Ransomware Attacks from 2016-2021

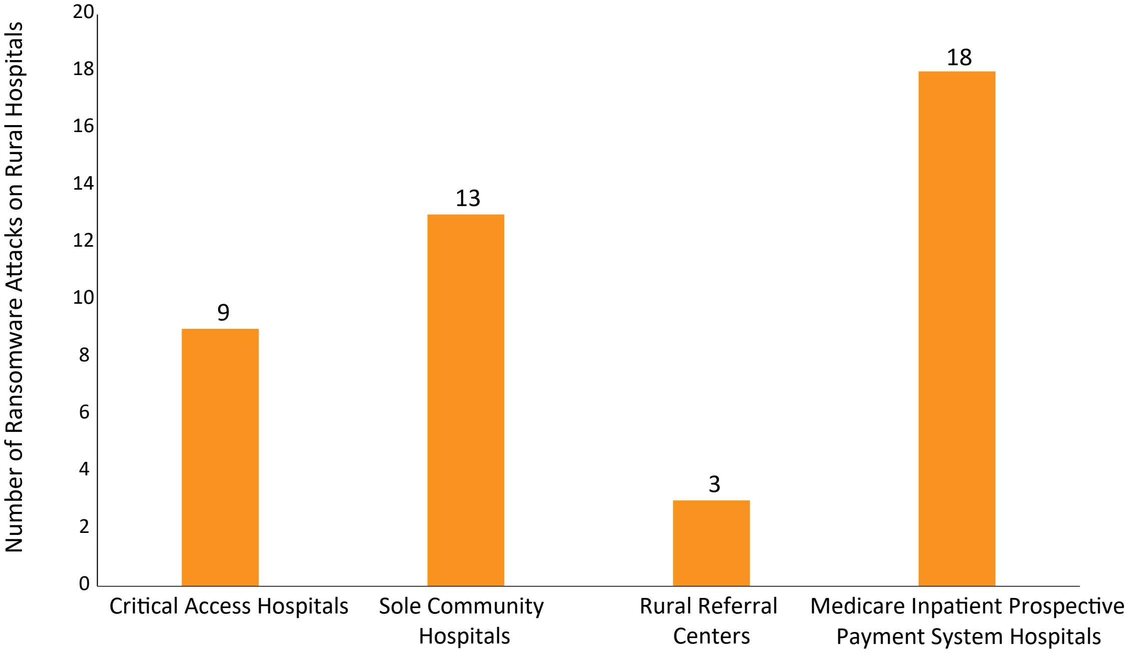
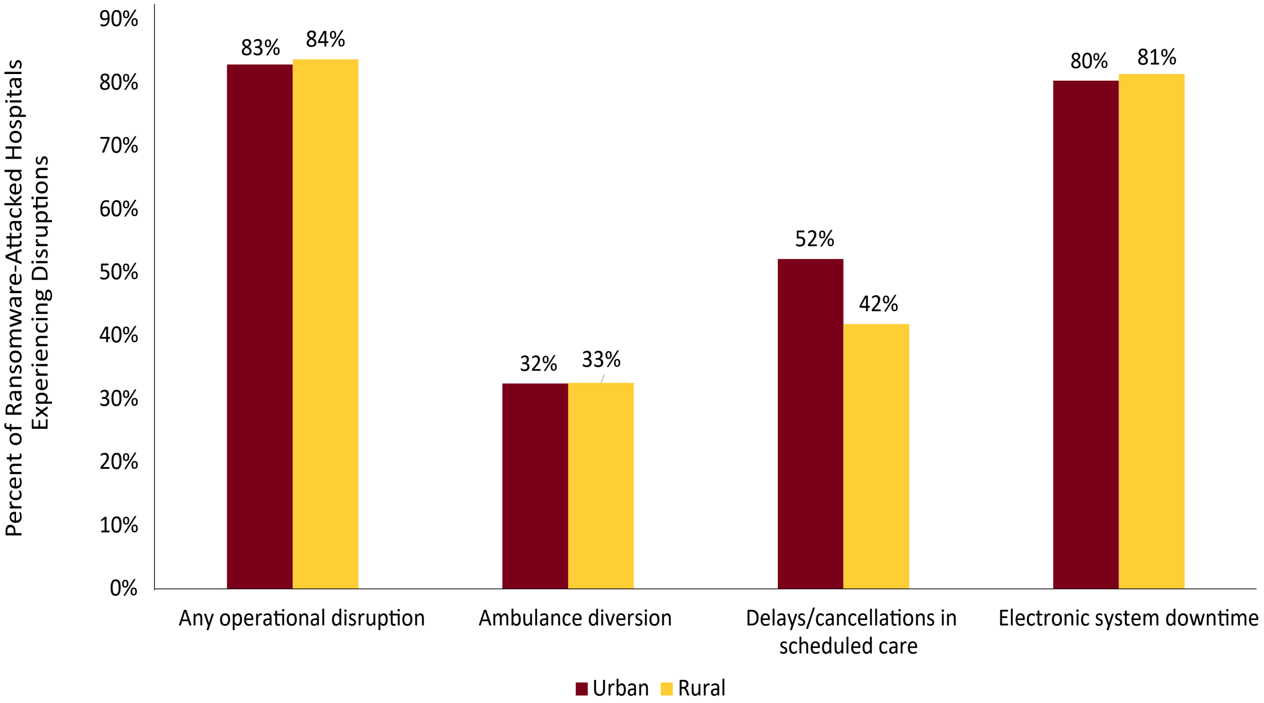


Figure 4 displays the frequency of operational disruptions during ransomware attacks on hospitals, by rural versus urban hospital location. Overall, the rate of operational disruptions from ransomware attacks was similar between rural and urban hospitals (84% and 83%, respectively). Electronic system downtime (e.g., inaccessible electronic health records) was the most common type of operational disruption, occurring for 81% of ransomware attacks on rural hospitals and 80% of ransomware attacks on urban hospitals. Ransomware attacks also resulted in the delay or cancellation of scheduled care for 42% of rural ransomware-attacked hospitals and 52% of urban ransomware-attacked hospitals. Ambulance diversion occurred during 33% of ransomware attacks on rural hospitals and 32% of ransomware attacks on urban hospitals.

Figure 4. Frequency of Operational Disruptions during Hospital Ransomware Attacks, by Rurality



Discussion and Implications

Past research shows that ransomware attacks on health care providers are increasing in frequency.[12] In this policy brief, we show that this phenomenon is not unique to urban areas, by documenting an increase in ransomware attacks on rural hospitals. From 2016 to 2021, ransomware attacks affected rural hospitals of all types, including Inpatient Prospective Payment System Hospitals, Critical Access Hospitals, Sole Community Hospitals, and Rural Referral Centers. The vast majority of ransomware attacks on rural hospitals resulted in some type of documented operational disruption, with electronic system downtime being the most common.

Our study has several limitations. First, we rely on the THREAT database to identify ransomware-attack hospitals. While this is the only available database for this purpose, we acknowledge the risk of omitting attacks that went unreported to HHS and uncovered in local or national news reports. Second, the THREAT database only allows observation of successful ransomware attacks, rather than attempted-and-thwarted ransomware attacks. The number of hospitals experiencing ransomware attack attempts (i.e., phishing emails, software security flaw exploits) is likely much larger than the number of hospitals experiencing ransomware attacks.

While the rates of operational disruptions caused by ransomware attacks was similar between rural and urban hospitals, rural hospitals face unique challenges in dealing with such disruptions and in combatting cybersecurity threats like ransomware attacks in the first place. Rural hospitals may be more susceptibile to common forms of cyberattack that exploit outdat-ed software with unpatched security flaws because of under-resourced IT infrastructure.[3-5] Compliance with recommended cybersecurity protocols can be quite costly, requiring scarce financial resources that many small rural hospitals may not have available.[6,7] Further, even with appropriate financial investments, rural hos-pitals face additional challenges hiring and retaining qualified information technology staff with cybersecu-rity expertise. Beyond preventing and addressing ransomware attacks, rural hospitals may face more serious consequences from operational disruptions, in the form of both patient outcomes and hospital finances. Rural residents have poorer underlying health and greater mortality, compared with urban residents.[18,19] Rural residents also have to travel further to reach their near-est hospital; ambulance diversions will increase these travel times even more for rural residents, an issue that is further complicated by limited (or nonexistent) ambulance services in many rural areas.[20,21] More research is needed to fully understand the unique impacts of ransomware attacks on rural hospitals and rural residents.

Overall, the combination of challenges for rural hospitals related to cybersecurity suggests that reducing the threat of ransomware attacks (and other cybersecurity threats) on rural facilities will likely necessitate policy solutions tailored to the needs and circumstances of rural hospitals, as they strive to provide high-quality care to their communities in an ever-changing 21st century landscape.

References

1.U.S. Department of Health & Human Services Office for Civil Rights. *FACT SHEET: Ransomware and HIPAA 2016* July 11, 2016.

2.Ransomware. 2021. (Accessed October 9, 2021 at https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware.)

3.Gabriel MH, Jones EB, Samy L, King J. Progress And Challenges: Implementation And Use Of Health Information Technology Among Critical-Access Hospitals. *Health Affairs* 2014;33:1262-70.

4.Office of the National Coordinator for Health Information Technology. *State and National Trends of Two-Factor Authentication for Non-Federal Acute Care Hospitals.* ONC Data Brief No 32 2015.

5.Heisey-Grove DM. Variation In Rural Health Information Technology Adoption And Use. *Health Affairs* 2016;35:365-70.

6.Levinson Z, Godwin J, Hulver S. *Rural Hospitals Face Renewed Financial Challenges, Especially in States That Have Not Expanded Medicaid*. KFF 2023.

7.Bai G, Yehia F, Chen W, Anderson GF. Varying Trends In The Financial Viability Of US Rural Hospitals, 2011–17. *Health Affairs* 2020;39:942-8.

8.Collier K. *An Illinois hospital is the first health care facility to link its closing to a ransomware attack*. NBC News 2023.

9.Martin L, Murphy M, Scanlon A, Naismith C, Clark D, Farouque O. Timely treatment for acute myocardial infarction and health outcomes: an integrative review of the literature. *Australian critical care : official journal of the Confederation of Australian Critical Care Nurses* 2014;27:111-8.

10.Joo YM, Chae MK, Hwang SY, et al. Impact of timely antibiotic administration on outcomes in patients with severe sepsis and septic shock in the emergency department. *Clin Exp Emerg Med* 2014;1:35-40.

11.Saver JL, Fonarow GC, Smith EE, et al. Time to Treatment With Intravenous Tissue Plasminogen Activator and Outcome From Acute Ischemic Stroke. *JAMA* 2013;309:2480-8.

12.Neprash HT, McGlave CC, Cross DA, et al. Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. *JAMA Health Forum* 2022;3:e224873-e.

13.McGlave CC, Nikpay SS, Henning-Smith C, Rydberg K, Neprash HT. Characteristics of Short-Term Acute Care Hospitals That Experienced a Ransomware Attack from 2016 to 2021. *Health Affairs Scholar* 2023.

14.Rural Hospital Cybersecurity Enhancement Act. US Senate 118th Congress. 118th Congress ed 2023.

15.Pierce K. *Testimony of Katherine (Kate) Pierce Former Chief Information Officer & Chief Information Security Officer, North Country Hospital and Current Senior Virtual Information Security Officer & Executive Director of Subsidy, Fortified Health Security Before the United States Senate Homeland Security & Government Affairs Committee* 2023.

16.Federal Office of Rural Health Policy (FORHP) Data Files. (Accessed December 31, 2021, at hrsa.gov/rural-health/about-us/what-is-rural/data-files.)

17.Office of Management and Budget. *OMB BULLETIN NO. 20-01: Revised Delineations of Metropolitan Statistical Areas, Micropolitan Statistical Areas, and Combined Statistical Areas, and Guidance on Uses of the Delineations of These Areas*. 2020.

18.Garcia MC, Rossen LM, Bastian B, et al. Potentially Excess Deaths from the Five Leading Causes of Death in Metropolitan and Nonmetropolitan Counties — United States, 2010–2017. *Morbidity and mortality weekly report Surveillance summaries (Washington, DC : 2002)* 2019;68 (No. SS-10):1-11.

19.Razzaghi H, Wang Y, Lu H, et al. Estimated County-Level Prevalence of Selected Underlying Medical Conditions Associated with Increased Risk for Severe COVID-19 Illness — United States, 2018. MMWR Morb Mortal Wkly Rep 2020;79:945-50.

20.Jonk Y, Milkowski C, Croll Z, Pearson K. Ambulance Deserts: Geographic Disparities in the Provision of Ambulance Services 2023.

21.Lam O, Broderick B, Toor S. *How far Americans live from the closest hospital differs by community type.* Pew Research Center 2018.

Suggested Citation

Neprash HT, McGlave CC, Rydberg K, and Henning-Smith C. Understanding the Rise of Ransomware Attacks on Rural Hospitals. *UMN Rural Health Research Center Policy Brief.* June 2024. https://rhrc.umn.edu/publication/understanding-the-rise-of-ransomware-at-tacks-on-rural-hospitals

This brief was revised in April 2025.

RHRC
Rural Health Research
& Policy Centers
Funded by the Federal Office of Rural Health Policy
www.ruralhealthresearch.org

Support for this study was provided by the Federal Office of Rural Health Policy, Health Resources and Services Administration, Cooperative Agreement U1CRH03717-13-00. The information, conclusions, and opinions expressed are those of the authors, and no endorsement by FORHP, HRSA, or HHS is intended or should be inferred.

For more information, contact Hannah Neprash (hneprash@umn.edu)

University of Minnesota Rural Health Research Center
Division of Health Policy and Management, School of Public Health
2221 University Avenue SE, #350 Minneapolis, MN, 55414