



Lakewood Health System in Staples, MN

Rural health resiliency

The rural hospital cybersecurity landscape

Erin Burchfield, Rachel Clark,
Laura Kreofsky

Rural hospitals are a cornerstone of healthcare delivery in the United States.

Introduction

Rural hospitals provide critical health services for nearly 14% of the U.S. population.¹ Many of these hospitals, however, are facing financial and operational strain. Coupled with aging technology, limited resources, and housing highly sensitive data, these hospitals have become a prime target for cyberattacks. This whitepaper explores the current state of rural hospitals, the unique cybersecurity threats they face, and the role technology companies can play to address both the immediate cyber risk and broader systemic challenges facing rural hospitals today.

Context – Rural Hospitals in the U.S.

Rural hospitals provide critical health services for roughly 46 million Americans, representing nearly 14% of the U.S. population.² Yet accessing health services can be difficult for rural residents, who must travel more than twice as far on average as urban residents to reach the nearest hospital.³

In addition to providing critical health services, rural hospitals play a vital role in local economies. Rural hospitals are often the largest employer in their community and attract businesses and investments to the area. A rural hospital's presence can be a decisive factor for families and individuals considering relocation to rural areas, enhancing local economic stability and growth. According to the American Hospital Association, "in 2020, rural hospitals supported one in every 12 rural jobs in the U.S."⁴ Overall, rural hospitals generate around \$220 billion annually in economic activity.⁵

The Problem – Rural Hospitals at Risk

There are roughly 2,000 rural hospitals across the country, comprising both public and private institutions.⁶ The viability of these hospitals is of national concern.

¹ Economic Research Service, U.S. Department of Agriculture, "[Rural Classifications – What is Rural?](#)," January 2025.

² Economic Research Service, U.S. Department of Agriculture, "[Rural Classifications – What is Rural?](#)," January 2025.

³ Pew Research Center, "[How far Americans live from the closest hospital differs by community type](#)," December 2018.

⁴ American Hospital Association, "[Rural Hospital Closures Threaten Access](#)," September 2022.

⁵ American Hospital Association, "[Rural Hospital Closures Threaten Access](#)," September 2022.

⁶ American Hospital Association, "[Fast Facts on U.S. Hospitals, 2025](#)," 2025.

However, from 2010-2017, rural hospitals were closing at a rate of about one per month.⁷ The velocity of closures continues: In 2020 and 2021 alone, there were a total of 136 closures.⁸ As of 2022, more than 429 rural hospitals are at high financial risk based on total margins and days cash on hand.⁹

With every hospital closure, rural residents must travel approximately 20 miles farther for common services, and 40 miles farther for specialized services.¹⁰ Increased travel distances are directly associated with higher mortality rates for time-sensitive conditions like heart attacks and strokes.¹¹ Hospital closures have a ripple effect on the broader healthcare ecosystem, driving increased burden on remaining providers who are often similarly under-resourced. Ultimately, each hospital closure exacerbates the growing disparity in health outcomes for rural Americans. Moreover, when a rural hospital closes, it leads to a 14% reduction in employment in the affected area, which can exacerbate pre-existing economic challenges.¹²

Resourcing Challenges

Rural hospitals often face dire financial situations driven by low operating margins, often due to lower patient volumes and high fixed costs relative to urban hospitals and exacerbated by lower reimbursement rates from insurers.

Compounding the financial resource strain, rural hospitals face significant challenges recruiting and retaining healthcare professionals. Finding skilled

staff in specialized areas of hospital management — for example, IT specialists or revenue management teams — is a significant challenge in rural areas. Moreover, rural hospitals face significant challenges recruiting and retaining healthcare professionals.

Finally, in large part due to limited budgets, rural hospitals are more likely to lack the resources to implement key cybersecurity measures, creating an ideal opportunity for exploitation from cybercriminals.

Cybersecurity Risks for Rural Hospitals

Rural hospitals often represent a unique opportunity for bad actors to exploit vulnerable, aging IT systems that house highly sensitive and valuable patient data. Studies have shown that small healthcare providers with under 500 employees suffer disproportionately compared to the broader healthcare sector.¹³

For rural hospitals, often already under financial strain, a ransomware attack may represent a tipping point.

Ransomware attacks pose a particular threat to hospitals, which are frequently

⁷ Politico, "[Healthcare's new rural frontier](#)," April 2017.

⁸ UNC, The Cecil G. Sheps Center for Health Services Research, "[195 Rural Hospital Closures and Conversions since January 2005](#)," 2005-Present.

⁹ Dobson DaVanzo & Associates, LLC, "[The Potential for Hospital System Integration to Improve the Financial Outlook of Rural Hospitals in the United States](#)," November 2024.

¹⁰ U.S. Government Accountability Office, "[Why Health Care Is Harder to Access in Rural America](#)," May 2023.

¹¹ Cornell University, Cornell Chronicle, "[Distance to nearest hospital is major factor in survival of heart attack victims, Cornell study shows](#)," February 2004.

¹² University of Pennsylvania, Penn LDI, "[Economic Impact of Rural Hospital Closures](#)," June 2022.

¹³ RiskIQ, "[RiskIQ Intelligence Brief: Ransomware in Health Sector 2020: A Perfect Storm of New Targets and Methods](#)," April 2020.

targeted by both financially motivated cybercriminals and nation-state threat groups. Hospitals often pay ransoms to avoid patient care disruptions, and malicious actors exploit this reality. According to an FBI report, the healthcare sector reported more ransomware attacks in 2023 than any of the other U.S. 16 critical infrastructure areas.^{14,15}

Moreover, these types of incidents surged by nearly 130% that year, according to reporting from the Office of the Director of National Intelligence (ODNI)¹⁶, on an already high baseline following Covid-19.

The rise of the “ransomware-as-a-service” (RaaS) ecosystem, where cybercriminals rent or sell their tools for a portion of the profits, has industrialized the cybercrime economy. This makes it easier for malicious cyber actors to use ready-made tools for their attacks.¹⁷

Among the most sophisticated financially motivated threat actors targeting healthcare is a group tracked by Microsoft as Vanilla Tempest. Active since July 2022, they use INC ransomware procured through RaaS providers to target U.S. healthcare, employing “double extortion,” to demand ransom for unlocking systems as well as prevent the release of stolen data.¹⁸

Other threat groups include Lace Tempest, Sangria Tempest, and Cadenza Tempest, each using various tactics like RaaS and double extortion. Threat actors often breach systems through phishing emails,

exploiting outdated software, and leveraging weak network security.¹⁹ Critical systems such as electronic health records, patient management systems, and medical devices are frequently compromised.

In a Microsoft analysis of 13 hospital systems, including rural hospitals, 93% of the malicious activity was related to phishing campaigns and ransomware, with most activity represented by email-based threats.

Email-based threats are among the most common entry point for stealing credentials or deploying malware leading to additional attacks. Attackers often exploit poor credential hygiene and legacy configurations to find easy entry points. Microsoft Threat Intelligence data shows attackers frequently exploit known vulnerabilities in software or systems that have patches or fixes available but remain unaddressed by many organizations.²⁰ Rural hospitals with aging IT systems and limited resources are often an easy target.

Rural hospital networks are also vulnerable to nation-state actors seeking strategic gain and posing a risk to national security. Government-sponsored hackers have used ransomware and collaborated with ransomware groups on tooling for

¹⁴ Federal Bureau of Investigation, “[Internet Crime Report](#),” 2023.

¹⁵ Axios, “[Health care was biggest victim of U.S. ransomware attacks last year](#),” March 2024.

¹⁶ Office of the Director of National Intelligence, “[Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double](#).”

¹⁷ Microsoft Threat Intelligence, “[Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself](#),” May 2022.

¹⁸ Microsoft Threat Intelligence, “[Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself](#),” May 2022.

¹⁹ NRHA, “[Cybersecurity: A path to increase rural health care preparedness](#).”

²⁰ Cybersecurity & Infrastructure Security Agency, “[Known Exploited Vulnerabilities Catalog](#).”

espionage purposes.²¹

Suspected Chinese government threat actors use ransomware tactics as a cover for espionage or disruption activity.²² Iranian threat actors have also been active targeting healthcare organizations. In August 2024, U.S. government agencies alerted the healthcare sector of Iran-based threat actor Lemon Sandstorm, which leveraged unauthorized network access to U.S. health care organizations to facilitate, execute and profit from ransomware attacks by apparently Russian-affiliated ransomware gangs.²³

Microsoft's Threat Intelligence teams track, assess, and disrupt both financially motivated and nation-state actors targeting critical sectors, including healthcare, to help mitigate such attacks. Through Microsoft's Digital Crimes Unit (DCU), we have taken both legal and technical action to disrupt cybercriminals and their facilitators, including those targeting healthcare institutions.^{24,25}

Microsoft's work in detecting, assessing, and disrupting actors like Vanilla Tempest and other financially motivated threat actors is a critical part of limiting the worst offenders' attacks; however, there is more work to be done supporting rural health by mitigating threats at the source. In 2025, Microsoft will focus efforts on stopping actors who seek to attack vital institutions, including health providers.

Governments in particular have a responsibility to stop attacks against hospitals. Governments have committed

to stop all cyberattacks on hospitals, healthcare, and medical research facilities, and on medical personnel and international public health organizations. It is time they finally do so and punish malicious actors who violate those rules.

Unless we act together, cyberattacks will continue to threaten the critical missions of rural hospitals. Recent data from the Texas Hospital Association reflects the continued growth and impact of cyberattacks nationwide.²⁶ In 2015, Texas experienced five data breaches through cyberattacks, exposing over 102,000 patient records. By 2022, there were 44 attacks exposing nearly 6 million patient records. This spike is not an anomaly, but the result of focused efforts to target hospitals who are simultaneously under-resourced with vulnerable IT environments, and housing valuable patient data.

Table 1: Texas Hospital Cyber Incidents/Impact by Year (Source: Texas Hospital Association²⁷)

Year	Incidents	Individuals Affected
2022	44	5,968,627
2021	35	5,551,575
2020	28	1,013,068
2019	21	2,279,951
2018	15	178,828
2017	20	598,902
2016	6	165,312
2015	5	102,668

²¹ American Hospital Association, "[Agencies alert health sector of Iranian and Russian cyber threats](#)," August 2024.

²² The Record, "[Suspected Chinese gov't hackers used ransomware as cover in attacks on Brazil presidency, Indian health org](#)," June 2024.

²³ American Hospital Association, "[Agencies alert health sector of Iranian and Russian cyber threats](#)," August 2024.

²⁴ Microsoft On the Issues, "[Notorious cybercrime gang's botnet disrupted](#)," April 2022.

²⁵ Microsoft On the Issues, "[Targeting the Cybercrime Supply Chain](#)," November 2024.

²⁶ Texas Hospital Association, "[Addressing The Surge of Texas Data Breach Rates](#)."

²⁷ Texas Hospital Association, "[Addressing The Surge of Texas Data Breach Rates](#)."

Impact of Cyberattacks on Rural Hospitals

Cyberattacks can have a devastating impact on rural hospitals. While service providers whose data or infrastructure was compromised are often seen as the primary targets, the direct victims of such attacks are healthcare professionals and patients. Cyber events can result in the suspension of hospital operations, affect emergency services and delay procedures. When a hospital is hit, lives are endangered. In fact, 20% of the hospitals that experienced a cyberattack reported an increase in patient mortality.²⁸

18.7

Reported average number of days in downtime following an attack, according to Comparitech²⁹.

The direct and indirect human impact of attacks on healthcare		
Patients	Healthcare professionals	Society
Delay in patient care	Stress and anxiety associated with incidence response	Erosion of trust in the healthcare sector – from hospitals to regulatory bodies and vaccine developers to public health authorities – associated with:
Endangering lives	Lack of access to medical devices and records	
Reduced patient safety	Revert to pen and paper	
Redirection to other facilities		
Inaccessibility of medical records and tests results		<ul style="list-style-type: none"> • handling of data confidentiality
Fear and sense of lack of control		<ul style="list-style-type: none"> • vulnerabilities exploited in code, software and hardware
Public release of personal information > risk of identity theft		<ul style="list-style-type: none"> • spread of disinformation
Loss of trust in the security of personal information		<ul style="list-style-type: none"> • low rate of prosecution

Figure 1: An overview of the direct and indirect human impact of cyberattacks on healthcare providers. (Source: The CyberPeace Institute³⁰)

²⁸ Tausight: Healthcare and Cybersecurity

²⁹ Comparitech, "On average, US healthcare organizations lose \$1.9 million per day to downtime from ransomware attacks," December 2024.

³⁰ The CyberPeace Institute, "Playing with Lives: Cyberattacks on Healthcare are Attacks on People," March 2021.

Cost per day for healthcare



\$1.9
million

Estimated amount lost by healthcare organizations on average per day of downtime following ransomware attack from 2018-2024, per Comparitech³².

It is not uncommon for hospitals' systems to be down for weeks following an attack, with the reported average downtime being 18.7 days.³¹ Although providers can revert to paper processes, this adds risk and cost to daily operations.

From a patient care perspective, hospitals dealing with a cyberattack face delays in diagnosis and treatment due to lack of access to diagnostic data. Non-emergency appointments and elective procedures are likely to be postponed or canceled. In addition to the disruption of medical services, patients can also suffer less visible impact including acute stress from being in this type of situation or psychological trauma and a sensation of powerlessness from having private information stolen and potentially exposed by criminals.

Recovery from cyberattacks, including expenses related to ransomware payment, system restoration, and service disruption, is often very costly. In 2023, according to an IBM report, data breach costs for healthcare rose to more than \$10.9 million.³³ For hospitals already experiencing financial strain, this can be the difference between solvency and shuttering.

As cyberattacks and data breaches in healthcare grow, and regulators require more robust protections, hospitals are finding themselves increasingly investing in cybersecurity.

³¹ Comparitech, "[On average, US healthcare organizations lose \\$1.9 million per day to downtime from ransomware attacks.](#)" December 2024.

³² Comparitech, "[On average, US healthcare organizations lose \\$1.9 million per day to downtime from ransomware attacks.](#)" December 2024.

³³ Vulcan citing IBM's "[Cost of a Data Breach Report.](#)" August 2023.



Spotlight: Sky Lakes Medical Center Cyberattack

Sky Lakes Medical Center is a 90-bed rural hospital serving 120,000 people across a 10,000-square-mile area in southern Oregon. The nearest hospital is 72 miles away. In 2020, Sky Lakes experienced a significant cyberattack with widespread impacts. The attack, which involved ransomware, encrypted the hospital's digital infrastructure, severely disrupting its clinical operations for 28 days. Staff reverted to paper documentation — during the downtime, the hospital ran through 60,000 sheets of paper.³⁴

The organization opted to not pay the ransom. Sky Lakes had to rebuild or replace 2,500 computers and clean its network to get back online.³⁵ Even after it hired extra staff, it took six months to input all the paper records into the system. The organization spent \$10 million.

In early September 2024, Microsoft Rural Health Program leaders met with Sky Lakes IT leaders to better understand the impact of the attack and gain insight to the needs of Rural Hospitals in avoiding cyber risks and responding to them when they do occur. Key takeaways included:

- Rural hospitals lack the technical resources and capabilities to monitor and manage an increasingly complex cyber ecosystem: "Out-of-the-box" managed solutions and services would be of high value.
- Rural hospital IT staff would benefit from standard playbooks of cyber best practices and incident response. Today, each hospital develops their approach and policies independently. Having best practice guidance would reduce the cognitive load during times of crisis.

³⁴ STAT, "[At small and rural hospitals, ransomware attacks are causing unprecedented crises](#)," April 2022.

³⁵ Politico, "[Health systems want government help fighting off hackers](#)," June 2022.

- Hospitals need support in moving systems to the cloud to reduce the cost and complexity of multiple backup environments.

The operational and financial strains of Sky Lakes because of the attack highlight the broader impact of cyberattacks on healthcare institutions, especially smaller and rural hospitals.

Addressing Rural Hospital Challenges – Technology Leaders’ Role

Healthcare has undergone a massive digital transformation over the last 20 years, with advances across a broad ecosystem of systems including electronic health records, business systems, platforms for data storage and transfer, telehealth platforms, and cybersecurity solutions and supporting federal policy. Rural hospitals have struggled to keep pace with the velocity and cost of change.

Technology companies can serve a vital role in supporting the overall resiliency of rural hospitals — not only through foundational cybersecurity support, but also innovation to address inefficiencies and cost drivers, IT skilling to ensure hospitals are prepared to manage these complex environments, and foundational internet infrastructure to enable telehealth access in the remote communities they serve. Partnerships and collaboration between hospitals, IT providers, and community organizations are key to long-term resiliency and adaptability in the face of rapid change.

Security Support: Microsoft Cybersecurity Program for Rural Hospitals

In 2024, Microsoft launched its Cybersecurity Program for Rural Hospitals. All rural hospitals in the U.S. are eligible to take advantage of the new Cybersecurity Program, which includes:

- Free security assessment offered through a pre-vetted Microsoft Security Partner to evaluate and identify strategies to mitigate a hospital’s cybersecurity risks;
- Curated learning pathways and resources to provide cyber awareness training for frontline staff and foundational cyber risk management certification to IT staff;

“Technology companies can serve a vital role in supporting the overall resiliency of rural hospitals.”

- One year of Windows 10 Extended Security Update at no cost, when available; and
- Security Product discounts and offers, including:



a. Independent Critical Access Hospitals and Rural Emergency Hospitals can access Microsoft nonprofit pricing (up to 75% off commercial price); and

b. Hospitals that are using O365 or M365 can get one year free of our most Advanced Security Suite, Microsoft 365 E5 Security and EMS E3, to ensure they can take action to secure their infrastructure immediately.

Microsoft Cybersecurity Program for Rural Hospitals

Program Status as of February 2025

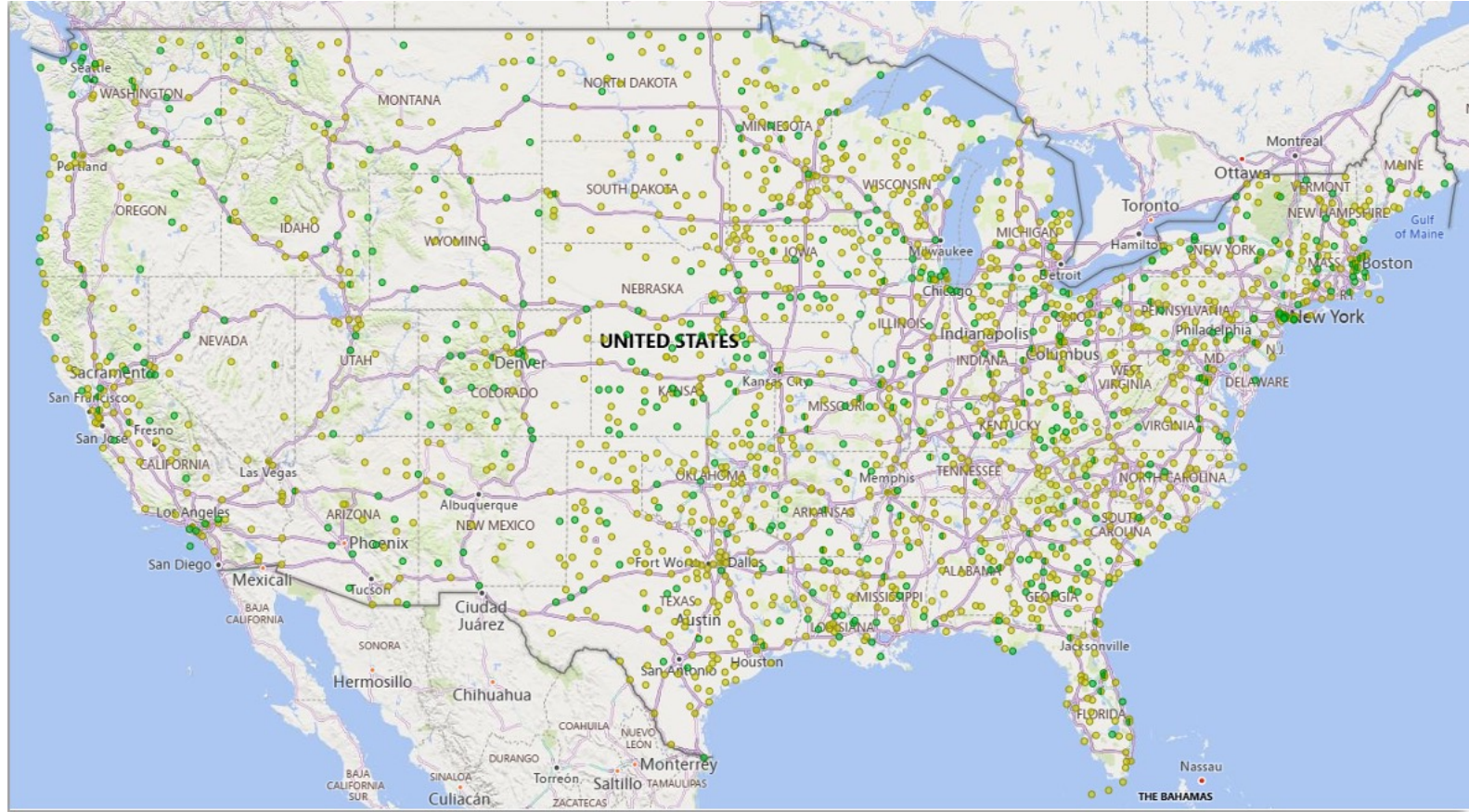
The initial response to the Microsoft program has exceeded projections, reflecting the level of need in rural hospitals. Since the program's launch, more than 550 rural hospitals from across the U.S. have registered. More than 375 hospitals are participating in Microsoft-funded cybersecurity assessments. Additionally, nearly 1,000 individuals

accessed cybersecurity training tailored to the needs of hospital front line and IT staff.

Early Program Findings

Microsoft, in coordination with its cybersecurity partners FSi Strategies and MorganFranklin Cyber, collated findings from over 250 completed assessments from rural hospitals across the U.S. This analysis identified areas of greatest vulnerability and risk. The preliminary data shows rural hospitals face significant threat exposure in the areas of:

- **Basic Cybersecurity Practices:** Most rural hospitals have struggled to implement basic cybersecurity best practices, including Email Security (65%), Multi-Factor Authentication (69%), Network Segmentation (62%) and Vendor/Supplier Cybersecurity Requirements (33%). This leaves rural hospitals substantially at risk across common threat vectors. IBM data shows that in 74% of breaches, human factors played a role, encompassing social



Source ● All rural hospitals ● Hospitals Registered

Figure 2: Rural hospitals in the U.S. and those participating in the Microsoft Cybersecurity Program for Rural Hospitals (as of January 15, 2025).

engineering tactics, mistakes, or misuse, with phishing being the leading initial attack vector, responsible for 41% of incidents.³⁶ Without basic best practices deployed, rural hospitals face considerable risk exposure.

- Mitigating Known Vulnerabilities: Running basic vulnerability scanning and doing timely patching according to an established process — is often neglected in rural hospitals, with only 43% of hospitals being deemed as receiving passing scores in these practices.
- Privileged Account Management is a top liability in many rural hospitals. Only 29% of rural hospitals adequately separate end-user and privileged accounts — or accounts with broader systems/data access. Often rural hospitals with lean IT

teams lack experience in developing and managing such policies and the capacity to do rigorous ongoing monitoring.

- While most rural hospitals scored well across the category of Asset Management, one sub-category, End-Point Management reveals substantial risk – less than 37% of assessed hospital met the expert-informed passing score.
- Training and Awareness: Most rural hospitals do not have a robust cybersecurity training and awareness program that educates the users on the types of cybersecurity risks there are most likely to experience. With some of the most common attack vectors being social engineering, this leads to a major security gap not just for the hospital, but for the employees, and awareness of security risks in their personal lives.

Rural hospitals face acute challenges across multiple fronts. Too often they face urgent “keep the doors open” needs.

A study conducted in early 2024 showed that rural healthcare leaders are most concerned about people management, revenue capture and digital capabilities. “Simmering” issues, including cybersecurity, are difficult to ignore, but still seemingly addressable only once

perceived higher-need, more urgent resourcing challenges are addressed.³⁷

Similarly, a 2024 study conducted by the Chartis Group revealed 50% of the nation’s rural hospitals are operating in the red, a significant jump from the 43% in 2023. States with the highest percentage of rural hospitals operating at a loss include Kansas (89%), New York and Wyoming (83% each), Vermont (75%), and Alabama (74%). In Kansas, which is home to 99 rural hospitals, the median operating margin is -10%.³⁸

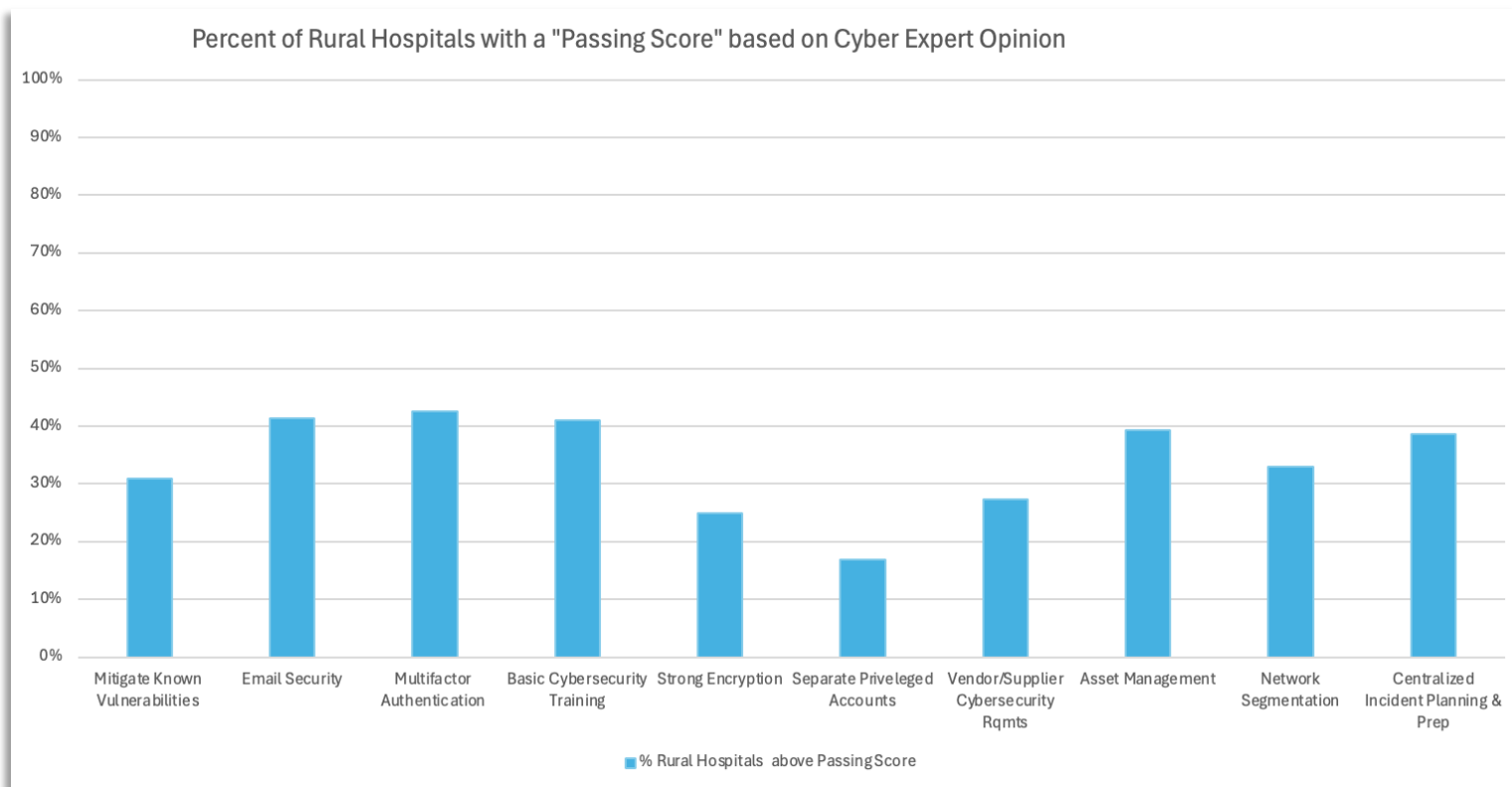


Figure 3: Percent of rural hospitals above “passing score” based on assessments conducted via Microsoft Cybersecurity Program for Rural Hospitals.

³⁷ Wipfli, “[State of Rural Healthcare: Research and outlook for 2024.](#)” 2024.

³⁸ Chartis, Chartis Center for Rural Health, “[Unrelenting Pressure Pushes Rural Safety Net Crisis into Uncharted Territory.](#)” 2024.

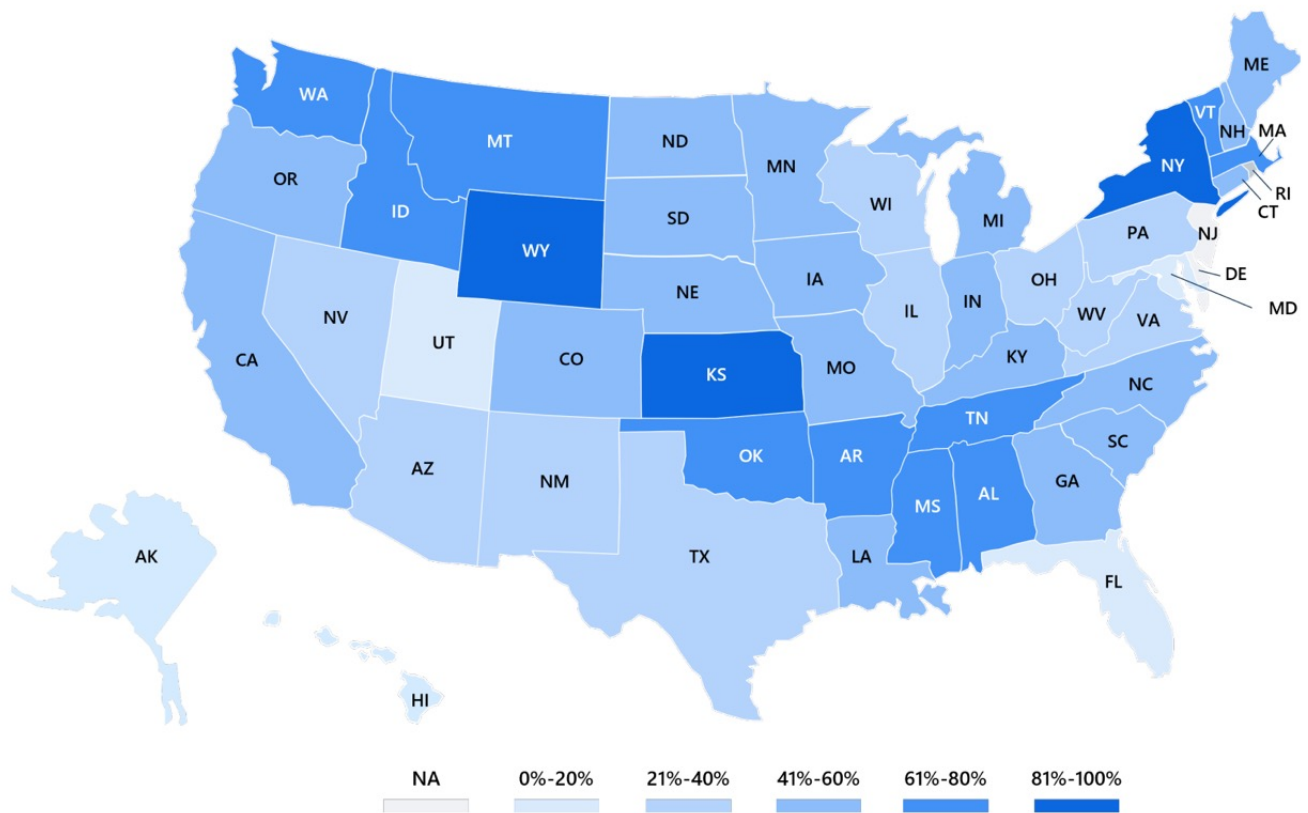


Figure 4: State-level percentage of rural hospitals with negative operating margin. (Source: Chartis³⁹)

To help address financial and operating challenges, innovation — and AI in particular — can play a compelling role and where technology companies can support rural hospitals and communities. By using generative AI to address underlying operational challenges, remove the “friction” of low-value work and documentation for staff and providers, and surface clinical insights frees scarce human resources to focus on other priorities and supports overall hospital viability.

Rural hospital financial viability depends on numerous factors — many unique to them. Factors such as lower patient volumes, higher fixed costs, and inability to drive economies of scale have all contributed to shrinking, if not negative, margins. Rural hospital finances are further stressed by low repayment rates from insurers. Continually changing prior authorization rules, higher

claim denial rates, and complex coding requirements from care providers contribute to lower reimbursement rates.⁴⁰

Compounding this, insurers are investing in more sophisticated tools and technology which further accelerate claim denials and creates even more coding complexity — particularly daunting for rural hospitals. Navigating this complexity requires investment in both people and process — something rural hospitals lack. As one rural hospital Chief Operating Officer (COO) pointed out, “we’re fighting algorithms with paper and spreadsheets.”⁴¹ This is where technology innovation can play a powerful role in leveling the playing field between large insurers and under-resourced rural hospitals.

³⁹ Chartis, Chartis Center for Rural Health, “[Unrelenting Pressure Pushes Rural Safety Net Crisis into Uncharted Territory](#),” 2024.

⁴⁰ Center for Healthcare Quality & Payment Reform, “[Preserving Access to Care in Rural Communities](#).”

⁴¹ Quote: Joseph (Bill) Rivera, Braden Health.

In spring 2024, Microsoft launched the Rural Health AI Lab (RHAIL), working side-by-side with rural healthcare leaders to collaboratively identify and co-design new tools leveraging generative AI to address unique needs of rural hospitals. A primary need identified by the participating hospitals was a tool to reduce the time and effort required to investigate and address denied insurance claims — one of the key drivers in low repayment rates.

In partnership with the RHAIL participating hospitals, Microsoft developed and deployed a generative AI tool that surfaces high-value recommendations for resolving the denied insurance claim. Ultimately, the tool will drive revenue recapture from insurers, helping to close the gap on insurance losses. The tool is deployed and being used at several early adopter hospitals, which are measuring efficacy in claims repayment and increases in staff productivity and revenue. Early-adopter hospitals include:

- Summit Healthcare in Show Low, AZ
- Aspirus Stanley in Stanley, WI
- Southern Coos Hospital in Bandon, OR
- Lakewood Health System in Staples, MN

This is just one example of how technology companies — and AI innovation — can play a new role in supporting rural hospitals and advancing rural health outcomes. Microsoft is committed to continuing our investments in the RHAIL project and delivering additional new technology solutions. Not only can innovation help hospitals alleviate

resourcing strain and inefficiencies, but those savings can help hospitals prioritize cyber risk remediation and become more secure.

Skilling and Workforce Development

Finally, a key area where tech companies are uniquely positioned to support rural hospitals is IT skilling, specifically skilling in cyber and AI. As of 2020, approximately 59% of cybersecurity teams across various sectors, including healthcare, were understaffed.⁴² This shortage is particularly acute in hospitals, where cybersecurity roles can take up to 70% longer to fill compared to other IT positions.⁴³ A study by Black Book and reported by Beckers Health IT found 75% of the Chief Information Security Officers (CISOs) surveyed noted experienced cybersecurity workers are unlikely to choose a career path in healthcare because of the potential ramifications after a cyberattack.⁴⁴

IT personnel with AI skills is even more difficult to source, a growing concern among hospital IT leaders. In 2023, 30% of hospital leaders had already recognized their lack of staffing with AI expertise.⁴⁵ These needs were repeatedly echoed by Critical Access Hospital executives attending the National Rural Health Association Annual Critical Access Hospital Conference in 2024. Microsoft spoke

⁴² ISACA, "[New ISACA Research: 59 Percent of Cybersecurity Teams are Understaffed](#)," October 2023.

⁴³ Black Book research report cited by Beckers Health IT, "[Why hospitals, health systems are facing a cybersecurity talent shortage](#)," November 2020.

⁴⁴ Black Book research report cited by Beckers Health IT, "[Why hospitals, health systems are facing a cybersecurity talent shortage](#)," November 2020.

⁴⁵ Definitive Healthcare, "[AI in healthcare study: A 2023 Definitive Healthcare special report](#)," November 2023.

directly with numerous leaders who noted AI and cyber training, skilling, and rural health career opportunities were critical needs.

Microsoft has a longstanding commitment to supporting rural IT skills development through programs such as Microsoft Tech Spark, which focuses on promoting digital skills and training for jobs of the future.

TechSpark also helps connect communities to broadband through the Airband Initiative, which offers high speed internet coverage through partnerships with local providers and nonprofits, helping serve the 157 million Americans who lack access to broadband.

Finally, programs like TechSpark provide a foundation for new initiatives to address the specific shortage of IT staff in rural hospitals. Along with policymakers, funders, and the health tech field, there is an opportunity to establish a new model to train, mentor and place career entrants into IT roles at rural hospitals. As one rural hospital CIO recently noted, he would like to see a “farm team” program provide a feeder into his hospital, which would not only support the hospital, but bring renewed opportunities to the local job market and economies of these rural communities.

Microsoft also recognizes that addressing rural health IT challenges requires a collaborative, community-based approach where CIOs, CTOs, and CISOs have a voice, venue and platform to problem-solve together. In partnership with Nordic Global and the College of Health

Information Executives (CHIME), Microsoft has launched the Rural Health IT Community.⁴⁶ This community has grown to over 300 members in just three months and provides rural health IT leaders a dedicated, enduring forum for establishing and articulating common needs, sharing best practices, and informing health IT vendors and policy makers.

Microsoft Engagement and Program Case Studies

Summit Health, Show Low, Arizona
Summit Health sits at the heart of the 10,000-square-mile Navajo County. Over 72% of county residents travel more than 40 miles to receive healthcare. The hospital serves a diverse patient mix, many with complex medical, behavioral health and/or substance abuse needs.

Summit has a relatively seasoned IT team actively monitoring and managing cyber risk. However, proactively hardening new/upgraded systems is a primary need for Summit: Correct security configuration is critical and not something smaller, less-resourced hospitals have expertise in, as reflected in Summit’s Cybersecurity risk assessment. As part of our comprehensive support, a Microsoft cyber service partner is working side-by-side with Summit Health staff to ensure its Azure configuration provides for optimal security and resiliency as it moves systems and data from on premise to cloud technology. This is enhancing patient data safety and building knowledge and skills.

⁴⁶ Beckers Health IT, [“Microsoft to create rural health IT community,”](#) September 2024.

Summit Health is also an early adopter of our initial Rural Health AI Lab (RHAIL) product—a generative AI tool used to help expedite research and resolution of denied insurance claims to drive revenue recapture and staff productivity.⁴⁷

Lakewood Health System, Minnesota
Lakewood is located in Staples, Minnesota, a town of roughly 3,000 people. The hospital is the surrounding communities' critical access hospital, meaning residents of the communities Lakewood serves would otherwise have to travel a significant distance to receive emergency or essential services.

Lakewood's team is all too familiar with the risks to its network posed by malicious cyber actors. Just a few years ago, the hospital experienced a spear-phishing incident in which the bad actor breached the hospital's email system. Lakewood's team responded quickly and carefully to resolve the issue, but risks to the hospital's networks remained.

Microsoft, a Microsoft security partner, and the Lakewood team embarked on a mission to bolster the security of the hospital's IT environment and mitigate cyber risk. In September 2024, Lakewood showed a "secure score" — measured through a model evaluating a hospital's policies, best practices, and technology tools for contemporary cybersecurity — of 19.5. By December of that year, Lakewood elevated its secure score to 47 — a significant improvement in just months. Such rapid change highlights Lakewood's diligence to implement security measures

and policies and their commitment to patient care. The implementation of Attack Surface Reduction (ASR) policies is the Lakewood team's next major step in its security journey with Microsoft. The team is also looking ahead at potential future projects, like the deployment of Azure ARC agents to on-prem servers for better management in Azure.

Finally, Lakewood's team leverages generative AI tools to improve the hospital's billing processes. With AI creating more efficient billing processes, Lakewood hopes to achieve better financial resilience — and more certainty in serving the community's patients.

Greenwood Leflore, Greenwood, Mississippi
For over 100 years, Greenwood LeFlore has served the region as a publicly owned healthcare organization. Over 40% of Mississippi rural hospitals are at risk of closing due to persistent financial challenges, and Greenwood LeFlore is one of them, nearly closing its doors in 2022. The hospital has since made positive steps toward improving its financial health.

Microsoft's Cybersecurity for Rural Hospitals Program assessment surfaced risks and recommendations for Greenwood LeFlore to improve cybersecurity and resilience. Microsoft's program is funding the deployment of tools like EntraID for identity management and multi-factor authentication (MFA). Microsoft is also supporting work to better track and manage privileged identity and access management, instituting security awareness training, and other activities essential for a contemporary mature cyber management program.

In June 2024, Congressman Bennie Thompson hosted a press release at Greenwood Leflore, promoting the program and Microsoft’s commitment to rural America — and the benefits the program would bring to the hospital and the community it serves.

Solving the Problem – A Collaborative Approach Is Needed

Addressing the current state of rural health requires a multifaceted approach, with meaningful engagement and support from public and private sectors. Tackling acute and accelerating cybersecurity risks faced by “target rich, resource poor” rural hospitals requires near-term action and resource mobilization, coupled with a broader focus on hospital resiliency, supported through innovation and partnerships.

A shared understanding of the severity and urgency of the problem is a primary step to mobilize funding and support. And a comprehensive approach to hospital resilience, including a focus on financial viability, resourcing, and capacity constraints, is the only way to ensure these hospitals remain open into the future.

Part 1: Addressing Near-Term Risk

Addressing basic cyber hygiene through tools and polices such as MFA, unified identity management and separation of user and privileged accounts, can address many high-probability pervasive risks.

Through our Cybersecurity Assessment

analysis, Microsoft’s Cybersecurity for Rural Hospitals Program has identified and prioritized those basic risks. Further, through collaboration with our cybersecurity partners, we estimated the cost to address and remediate those top risks and ensure a rural hospital receives a “passing” score. Based on average IT footprint, our partners estimate the

“Addressing the current state of rural health requires a multifaceted approach.”

required baseline is approximately \$30,000-\$40,000 per independent rural hospital with approximately 50 beds and 200 end users.

There are approximately 1,000 independent rural hospitals, which are not part of a larger hospital network or system where IT solutions are often deployed across the network. By addressing the top vulnerabilities among the 1,000 independent — and often among the most vulnerable — rural hospitals, a significant portion of risk can be mitigated. The cost to achieve this outcome would be roughly \$40-45 million USD. Applying that cost across the entire landscape of 2,100 rural hospitals in the U.S., the cost to address these acute, near-term risks totals roughly \$70-75 million.

Part 2: Ensuring hospital resilience into the future

A one-time remediation of the most critical cybersecurity risks to rural hospitals is critically important to help hospitals stay as safe as possible in the near term.

However, this stop-gap measure is not entirely sufficient. As AHA President and CEO Rick Pollack noted at the launch of the Microsoft Cybersecurity Program for Rural Hospitals: “Cybersecurity is a top priority for America’s hospitals and health systems. It is also a shared responsibility ... It’s no secret that many rural hospitals across America are struggling as they serve as a health care lifeline in their communities so keeping them safe is essential.”⁴⁷


There is a compelling need for the healthcare industry, policymakers and funders, and technology companies to bolster resourcing and innovation across rural areas. Microsoft is committed to this effort and looks forward to working with public and private sector partners to advance a collaborative response in rural America.

Conclusion

Rural hospitals are vital points of care for millions of Americans and a cornerstone in rural communities. Unfortunately, cybersecurity is a growing threat to their overall viability. There is an urgent need for both immediate and sustained support for these essential institutions.

Microsoft envisions, through collaboration with the private-sector and public-sector partners, a near-term targeted effort, coupled with broader remediation as well as sustained support to ensure long-term rural hospital resilience. Through this partnership and sustained commitment to rural America, we can take action at an unprecedented scale and speed to mitigate cyber risk, drive innovation, and ensure both rural hospitals and the Americans they serve are resilient into the future.

Appendix: Additional In- Depth Engagements



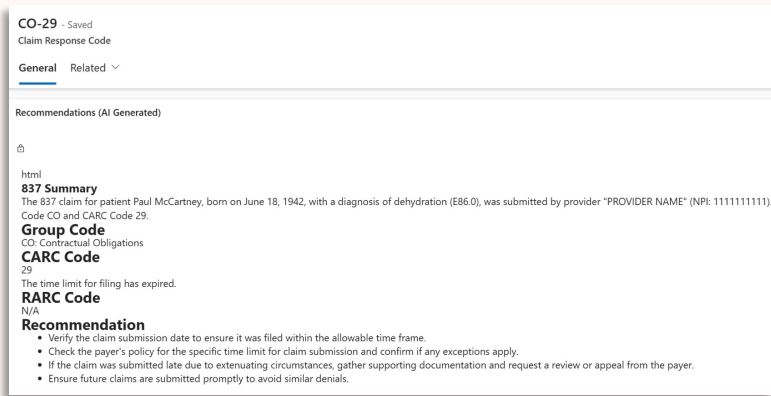
In addition to offering Microsoft-funded cybersecurity risk assessments to all rural hospitals in the United States, Microsoft and FSi Strategies are partnering with 12 representative rural hospitals across the U.S. to provide direct, hands-on cyber risk remediation and solutions. These partnerships will inform best practices across the end-to-end cyber remediation process, from assessment to addressing areas of risk.

Notably, the work with these hospitals has significantly accelerated their ability to implement much-needed cyber risk management tools. The Director of Information Systems at Greenwood Leflore Hospital stated that addressing the top risks in their assessment would have taken at least 18-24 months to start, given severe capacity constraints of their small hospital IT department. Similarly, at Lakewood Hospital, these fast-tracked services are allowed the hospital to expedite implementation of needed cybersecurity tools from 6-8 months to 10-12 weeks.

Table 2: Hospital In-Depth Engagements

Hospital	City, State	Hospital	City, State
Aspirus Stanley	Stanley, WI	Houston County Community Hospital	Erin, TN
Field Health System	Centreville, MS	Lakewood Health System	Staples, MN
Fulton County Medical Center	McConnellsburg, PA	St James Parish Hospital	Lutcher, LA
Greenwood Leflore	Greenwood, MS	Southern Coos Hospital	Coos Bay, OR
Haywood County Community Hospital	Brownsville, TN	Summit Healthcare	Show Low, AZ
Henderson County Community Hospital	Lexington, TN		

Appendix: AI Innovation Details



Source: Microsoft Cybersecurity for Rural Hospitals Program

Through an iterative design and testing process which involved the RHAIL participating rural hospitals' business and IT staff, Microsoft developed and deployed a Copilot tool built on Azure and PowerApps that surfaces high value recommendations for resolving the denied insurance claim. Azure AI analyzes and creates the recommendations while the Power App serves it up to users in a clean, easy to use interface.

The goals of the tool include helping drive workflow efficiency, lowering hospital accounts receivable, and driving full revenue capture from insurers.

Additionally, early users of the tool are excited by how it can be used to address workforce challenges through supporting easier billing staff onboarding and training with a "virtual assistant". Deployment is underway at Lakewood Health, Southern Coos Hospital, Aspirus Stanley Hospital, and Summit Health. Key metrics are being tracked to ascertain the adoption and value of the tool, including:

- Usage time by individual billing staff member;
- User rating of AI generated recommendations in terms of utility and accuracy;
- Average time to "work a claim" in the tool vs. traditional manual Workqueue methods; and
- Subject Matter Expert (SME) evaluation of impact on days in A/R and percent of claims resolved.



©2025 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.