Cybersecurity Strategies for Rural & Critical Access Hospitals

A Comprehensive Resource Guide

CloudWave

INTRODUCTION

Rural and critical access hospitals face a mounting challenge in delivering quality healthcare services to their communities: cybersecurity threats. Limited resources, the rapidly changing threat landscape, and evolving regulatory requirements are making the situation even more difficult for these hospitals. The consequences of cyberattacks can be devastating, disrupting patient care and compromising safety.

This guide offers practical resources to help rural and critical access hospitals better understand, prepare for, and combat cyberattacks, including:

- The alarming reality of cyberattacks in rural healthcare
- The financial and operational toll of cyberattacks
- Information on how to develop a comprehensive cybersecurity strategy to enhance their cybersecurity posture
- Tips on how to offer a culture of cybersecurity awareness and prioritize patient-centric cybersecurity

By taking proactive steps to strengthen cybersecurity defenses, rural and critical access hospitals can protect patient care, ensure continuity of services and care during cyberattacks, and ultimately fulfill their mission to safeguard their communities.

How to use this guide:

To get the most out of this guide, we recommend:

1. Using the **interactive table of contents** to navigate to specific topics of interest
2. Reviewing the **action icons** throughout the guide, which provide tips, advice, and best practices for implementing cybersecurity strategies
3. **Sharing this guide with your team** and using it as a starting point for discussions and planning around cybersecurity

TABLE OF CONTENTS

WHY RURAL AND CRITICAL ACCESS HOSPITALS ARE AT A HIGHER RISK FOR CYBERATTACKS

Rural and critical access hospitals face unique obstacles in delivering healthcare services to their communities. One challenge continues to grow: **cybersecurity attacks that can disrupt patient care and have devastating consequences**.

Cybersecurity threats are a mounting concern for healthcare organizations nationwide, but rural and critical access hospitals are particularly at risk. With limited budgets, IT resources, and untrained staff, these hospitals often struggle to defend against increasingly sophisticated attacks.

AN ALARMING REALITY

60%

of rural hospitals have **experienced a cyber incident** in the last three years[1]

The nation's roughly 1,800 rural community hospitals are among the **most vulnerable** to dangerous attacks[2]

The operational disruptions of attacks may have a **greater effect on financially vulnerable rural hospitals** and their patients[3]

CYBERATTACKS PUT PATIENT SAFETY AT RISK

70%

Nearly 70% of healthcare organizations hit by cyberattacks **report patient care disruptions**.[4]

Among the organizations that faced four common types of cyberattacks[5]

56%
reported **poor patient outcomes** due to care delays

23%
experienced an **increase in procedure complications**

28%
said patient **mortality rates rose**

THE FINANCIAL TOLL OF CYBERATTACKS

$7.42M

The **average healthcare data breach** reached $7.42 million per incident in 2024[6]

$500K+

Over three-quarters of healthcare organizations reported **paying more than $500,000 in ransom** as a result of cyberattacks[7]

$1.9M

Hospitals **lose** an average of $1.9 million **per day** during ransomware-related downtime[8]

18 Days
The typical attack can leave hospitals **without access to electronic systems** for up to 18 days[9]

46%
of rural hospitals currently **operate with a negative margin**[10]

756
rural hospitals are currently **at risk of closure** due to financial problems[11]

Today's rural hospital systems **cannot afford the financial impact** of shutting services down due to inaccessible records while servers are down, or paying the ransom[12]

RURAL HOSPITAL-SPECIFIC IMPACT

During the first week of a ransomware attack,

↓14.7%
inpatient admissions at rural hospitals dropped

↓35.3%
outpatient visits fell

↓10%
ER visits declined[13]

4-7x
When a rural hospital goes down, the nearest unaffected hospital is more than 30 minutes away on average—**four to seven times further than for urban hospitals**[14]

5 → 17
The number of rural hospitals experiencing **ransomware attacks more than tripled** from 2016 to 2021, increasing from 5 to 17 per year[15]

2-3 weeks
Recovery to pre-attack volume and revenue levels typically took two to three weeks for both rural and urban hospitals[16]

182
rural hospitals have closed or converted away from inpatient care since 2010[17]

THE STRUGGLE TO KEEP UP: RURAL HOSPITALS ARE UNDERPREPARED AND UNDERSTAFFED

A 2023 HIMSS Healthcare Cybersecurity Survey reported[18]

74%
that **recruiting qualified cybersecurity professionals was a significant workforce challenge** for 74% of respondents

47%
indicated that the **lack of cybersecurity-related experience** or skills was a challenge in hiring cybersecurity professionals

43%
also indicated that their organizations **lack sufficient budget** to hire qualified healthcare cybersecurity professionals

Lack a full-time cybersecurity employee
A significant proportion of rural critical access hospitals **lack even a single full-time employee dedicated to cybersecurity**[19]

279 Days
Healthcare **breaches** take an average of 279 days to **identify and contain**—the longest of any industry[20]

HEALTHCARE CYBERSECURITY PERSPECTIVES

CloudWave Thought Leaders Share their Thoughts and Strategies

Increased Regulations and Funding Continue to Impact Healthcare

As increasing cyberattacks continue to plague the healthcare industry, hospitals and health systems must take the measures necessary to prevent unauthorized access to their critical systems and patients. The regulatory and funding landscape is evolving rapidly, with new federal initiatives and requirements designed to strengthen healthcare cybersecurity.

The $50 Billion Rural Health Transformation Program

Beginning in 2026, the federal government's Rural Health Transformation Program will provide $50 billion to modernize rural healthcare infrastructure across all 50 states. Each state will receive funding, averaging $200 million in year one and continuing through 2030, to strengthen care delivery for the 46 million Americans who rely on rural health systems.

Key Program Elements:

- Half of the funds will be distributed equally across all approved states
- The remaining 50% will be allocated based on rural health needs, including population dynamics, workforce shortages, and community health indicators
- Infrastructure modernization explicitly includes cybersecurity improvements, data sharing capabilities, and digital health tools
- States can invest in technology-enabled care, telehealth expansion, workforce development, and evidence-based interventions

Why This Matters for Cybersecurity:

Digital transformation sits at the center of rural healthcare's future, and cybersecurity is the foundation that enables every modern care delivery initiative. Rural hospitals that prepare now by assessing their risks, documenting their needs, and building strategic cybersecurity roadmaps will be best positioned to compete for support when states begin allocating funds.

Preparation Steps for Rural Hospitals:

- Conduct a comprehensive cybersecurity and HIPAA risk assessment to establish a clear picture of your current security posture
- Strengthen core cybersecurity fundamentals, including MFA, network segmentation, email security, and backup/recovery readiness
- Build a funding-ready cybersecurity roadmap outlining priority projects, timelines, estimated budgets, and expected impacts on patient care
- Document how cybersecurity improvements support broader transformation goals like telehealth expansion and digital health adoption

Evolving HIPAA Requirements

The regulatory landscape for healthcare cybersecurity is evolving rapidly. Key developments include:

Proposed 72-Hour Breach Notification Rule:

HHS has proposed requiring covered entities to notify HHS of breaches affecting 500 or more individuals within 72 hours of discovery, significantly shortened from the current 60-day requirement. This accelerated timeline emphasizes the critical need for rapid incident detection and response capabilities.

Other Key Regulatory Developments:

- Enhanced Business Associate Oversight: New requirements emphasize stronger vendor risk management and supply chain security assessments
- Incident Response Planning: Federal agencies are emphasizing the need for comprehensive, tested incident response plans that prioritize patient care continuity
- Cybersecurity Performance Goals: The Healthcare and Public Health (HPH) Sector-Specific Cybersecurity Performance Goals provide a framework for strengthening security across healthcare organizations

State-Level Cybersecurity Initiatives

States are taking independent action to strengthen healthcare cybersecurity. Recent examples include:

- Comprehensive cybersecurity regulations requiring hospitals to implement robust infrastructure to prevent cyberattacks
- Mandatory policies for evaluating and testing the security of third-party applications
- Requirements to develop incident response plans and perform regular testing to ensure patient care continuity during disruptions
- State-level funding allocations to help hospitals upgrade technology systems to meet cybersecurity requirements
- Immediate reporting obligations for cybersecurity incidents to state health departments

The Proactive Approach:

Collaboration between stakeholders and industry players will be essential as regulations rise to ensure that all healthcare facilities, regardless of size, can meet and exceed the cybersecurity standards necessary in today's threat landscape. Companies offering cybersecurity solutions and services are stepping up to help healthcare organizations meet regulatory requirements and identify the most effective strategies to maximize state and federal funding.

Even if your state hasn't enacted specific regulations, hospitals should not wait to implement improved processes and strategies. Those who act now will be in a better position should their state pass legislation, and will be better protected from cyber attackers.

The FBI's 'Threat to Life' Designation

The FBI and DOJ are now treating the patient and public safety risk that cyberattacks pose on hospitals as a 'threat to life' crime.

This designation reflects the growing recognition that cyberattacks on healthcare facilities are not merely data breaches but direct threats to patient safety and lives. This further reinforces the need to prioritize patient safety and uphold quality of care during cybersecurity incidents. Instead of the traditional IT approach to protecting data, there must be a shift to protecting patients first and foremost in an effective cybersecurity approach.

Even if your state hasn't enacted specific regulations, hospitals should not wait to implement improved processes and strategies. Those who act now will be in a better position should their state pass legislation, and will be better protected from cyber attackers.

Engineers Corner: An Attackers' Perspective on Cybersecurity Exploits

With healthcare cyberattacks becoming more frequent and sophisticated, staying informed and prepared is critical. The knowledge and strategies needed to defend against these emerging threats and ensure the security of your healthcare IT infrastructure include an understanding of the following:

- The latest attacker tactics
- Advanced persistent threats targeting firmware to maintain long-term control over systems
- How these attacks impact healthcare and critical infrastructure
- Why traditional penetration testing may no longer be sufficient

SSH Compromise (CVE-2024-3094) Impacting Linux

Unless an attacker performs a bot attack, they will likely start with passive reconnaissance because it's easy to do and follow up with vulnerability scanning. In addition to keeping patches updated, organizations should consider how to shut down external-facing systems if there is an SSH compromise. Being proactive and treating the perimeter as the last line of defense is critical in these situations.

How To Find Where Vulnerabilities Exist:

Initial Research

Examine the code. Hackers can purchase any technology an organization owns, including switches, EHRs, and more. Look at all documentation available for a product.

Source Code Review

This includes static, fuzzy, and dynamic review and testing. Tools are getting better at identifying where vulnerabilities may exist, and some are starting to employ AI to enhance their functionality.

Once a potential vulnerability is identified, attackers must determine if it's exploitable. Although determining where an exploit exists in the source code or system still requires some engineering capabilities, tools are getting better at pointing out the location.

Some software engineers must consider input validation more comprehensively, including at the backend. The basic rule for writing secure systems is any input should be sanitized and have clear fallbacks if inappropriate data is passed.

Furthermore, several vulnerable areas keep emerging, including input validation accounts. When dealing with critical infrastructure systems, ask if partners follow OWASP and what practices are in place to address these security issues.

The Vicious Nature of BIOS Attacks

At the BIOS level, attackers can interact with or intercept everything that happens in that system. They run below the operating system (OS) and can inject into and take over any process, command, data exchange, or network connectivity. These attacks are particularly dangerous for healthcare's critical infrastructure and medical devices as they can lead to persistent, hard-to-detect infections that compromise the integrity and functionality of essential systems.

- BIOS attackers also turn off protections like firewalls and antivirus tools. Relying on integrity checks or secure boots, in that case, creates a false sense of security.
- Many BIOS attacks stay hidden and use timer-based deployments.
- Getting to the BIOS to install the exploit is trickier as the attacker may wait until a reboot occurs. From there, every keystroke can be logged, and each mouse movement is examined.

Mitigating Attacks from Midnight Blizzard

A group called Midnight Blizzard (aka, APT29 or Cozy Bear) has been implicated in firmware attacks. There are ways for organizations to defend themselves, including:

- **Regular firmware updates:** Keep firmware updated with patches from trusted vendors. Create a process and reminders within your organization to know when to review firmware. Check for manufacturer updates and inventory what firmware versions are running, especially in medical devices and IoT systems.
- **Enable secure boot:** Configure secure boot to ensure only trusted firmware OS components are loaded during startup.
- **Hardware-based security:** Utilize trusted platform modules (TPMs) to ensure firmware integrity and prevent unauthorized access.
- **Firmware integrity monitoring:** Deploy tools capable of monitoring and verifying integrity to detect unauthorized changes.
- **Restrict administrative privileges:** Service accounts granted admin privileges are a source of vulnerability. Limit administrative privileges and monitor for privilege escalation attempts to prevent unauthorized firmware updates.

Oracle Weblogic Server OS Command Injection

The first step in this attack is making a malicious HTTP request, setting up the underlying environment to allow the attacker to bypass security, and then uploading or sending an XML file to give someone nefarious command execution capabilities.

This works because of how the code is implemented. A malicious payload can be embedded within a SOAP envelope, and once this passes through to the backend system, an attacker controls it.

Typically, reverse commands are used that allow the system to call back. The attacker then gives an IP address or a hostname to establish a reverse tunnel and gain access at an admin level. In this case, even if the server is shut off, network connectivity for the attack is preserved.

Limitations of Traditional Penetration Testing

Penetration (pen) testing is one defense an organization uses to test its security. However, the traditional approach is becoming insufficient against sophisticated cyber threats as most pen testing methods are outdated, performing some service level analysis but overlooking more sophisticated approaches—and rarely looking at firmware and BIOS attacks. Additionally, many tests are not tailored to the healthcare sector and focus primarily on meeting compliance and regulatory rules.

A modernized, comprehensive approach is required to effectively protect sensitive patient data and ensure the integrity of healthcare services. Healthcare organizations should utilize continuous security assessment and consider the following:

Advanced threat simulation

This includes red team exercises, attack surface management, and attack dissection.

Firmware updates and hardware security

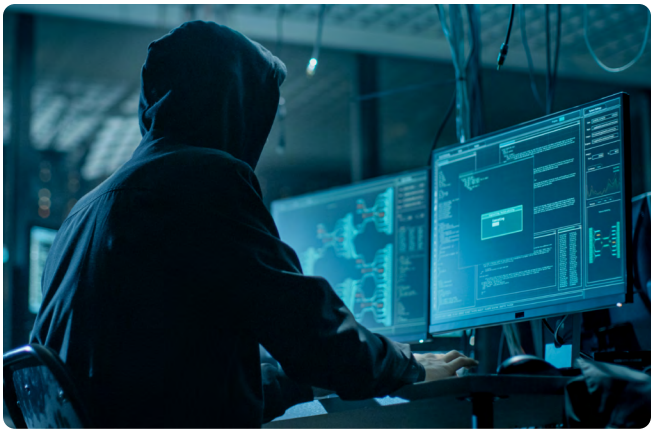
Can someone get into the hardware through firmware? What would that mean?

Comprehensive internal and external testing

As the sophistication of pen testing increases, it will probably be more expensive and time-consuming. Pick a few critical systems, like EHR or domain controller, and go deep into them.

If a healthcare organization is hit with a true cyberattack, critical patient care systems must become operational as quickly as possible, including the domain controller, EHR, lab, pharmacy, and portals. Understanding how well those systems can withstand a proper pen test attack dissection is critical.

To explore this critical subject in more detail, read the complete blog post here or listen to the on-demand webinar, "An In-Depth Look at Cyber Exploits from the Attackers Perspective," provided to our CloudWave Cybersecurity Insider Program members.



Practical Steps for Meeting the New Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals

The Healthcare and Public Health (HPH) Sector-Specific Cybersecurity Performance Goals (CPGs) are designed to strengthen cybersecurity across the healthcare sector, assist healthcare organizations in implementing high-impact cybersecurity practices, fortify healthcare organizations' resilience, and ultimately protect patient safety.

Attacks have continually been the cause of disruption and delay in care delivery. Instead of the traditional IT approach to protecting data, there must be a shift to protecting patients first in an effective cybersecurity response, and the new HPH CPGs are a positive step toward achieving this.

The HPH CPGs address the common attack vectors against U.S. hospitals quantified in the Hospital Cyber Resiliency Landscape Analysis report. The report notes that The National Security Council considers the HPH sector one of the top three sectors prioritized for additional cybersecurity attention as the increase in devastating ransomware and other cyberattacks continues to grow in both numbers and severity. These repeated attacks have continually been the cause of disruption and delay in care delivery, creating an unprecedented risk to patient safety. In fact, the FBI and DOJ are now treating the patient and public safety risk that cyberattacks pose on hospitals as a "threat to life" crime.

This further reinforces the need to prioritize patient safety and uphold quality of care during cybersecurity incidents. Instead of the traditional IT approach to protecting data, there must be a shift to protecting patients first and foremost in an effective cybersecurity response, and the new HPH CPGs are a positive step toward achieving this.

> The FBI and DOJ are now treating the patient and public safety risk that cyberattacks pose on hospitals as a "threat to life" crime.

Top 10 Sectors by Intrusion Frequency

- HEALTHCARE
- TECHNOLOGY
- FINANCIAL
- TELECOMMUNICATIONS
- RETAIL
- MANUFACTURING
- ACADEMIC
- SERVICES
- GOVERNMENT
- PHARMACEUTICAL

Below is a three-step process designed to help healthcare organizations more effectively adopt and meet cybersecurity performance goals.

STEP 1

Implementing Critical Best Practices

As a starting point, we identified the critical best practices in successfully defending a healthcare organization against cyber threats. These are not the named HPH CPGs, but the elements below serve as a foundational checklist for guiding healthcare organizations in aligning with the evolving industry standards and expectations for legal defensibility.

The most advanced hospitals with the most mature security programs are deploying and embracing an advanced set of tools, including:

- Encryption
- Intrusion and Detection Prevention Systems
- Network Monitoring and Analytics
- Security Information and Event Management
- Next-Generation Endpoint Protection
- Data Loss Prevention
- Network Segmentation
- Cloud Access Security Broker

Building on this foundation, we will now outline the two types of goals identified in the HPH CPGs: essential (foundational goals that your organization should be pursuing) and enhanced (goals your organization should aim to implement if it is not already doing so).

STEP 2

Essential Goals

- Mitigate Known Vulnerabilities
- Email Security
- Multifactor Authentication
- Basic Cybersecurity Training
- Strong Encryption
- Basic Incident Planning and Preparedness
- Revoke Credentials for Departing Workforce Members, Including Employees, Contractors, Affiliates, and Volunteers
- Unique Credentials
- Separate User and Privileged Accounts
- Vendor/Supplier Cybersecurity Requirements

STEP 3

Enhanced Goals

- Asset Inventory (Including Medical Devices)
- Third-Party Vulnerability Disclosure
- Third-Party Incident Reporting
- Cybersecurity Testing (Including Pen Testing and Application Security Testing)
- Cybersecurity Mitigation
- Network Segmentation
- Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures (Network Intrusion Detection, Honeypots, etc.)
- Centralized Log Collection
- Centralized Incident Planning and Preparedness
- Configuration Management

This step-by-step progression not only helps in achieving the HPH CPGs but also in maintaining a clear and measurable path toward improvement.

We recommend organizing the CPGs into a framework to create an effective plan for how your organization is meeting or will meet the performance goals. This includes the categories of maturity, plan (to get there), cost, and status. In terms of measuring maturity, do a thorough assessment as to where your organization stands with reaching the HPH performance goals in four different layers:

- Not implemented
- Partially implemented
- Largely implemented
- Fully implemented

Implementing these strategies requires a carefully planned approach, ensuring that each layer of maturity is comprehensively evaluated and addressed. By systematically advancing through the stages of implementation, your organization can progressively enhance its cybersecurity posture.

This step-by-step progression not only helps in achieving the HPH CPGs but also in maintaining a clear and measurable path toward improvement. Effective implementation also includes continuous monitoring and adjustment to align with evolving cybersecurity threats and organizational changes. If you don't know how to get started identifying your maturity or don't have the resources to do it, check out our Cybersecurity Capability Maturity Model that identifies gaps, helps you prioritize, and tracks progress over time.

While not presently mandated, the HHS' Healthcare and Public Health Cybersecurity Performance Goals serve as a remarkable framework that can help strengthen a healthcare organization's cybersecurity posture and influence legal perspectives. Engaging in proactive discussions and strategizing around the HPH goals is essential in advancing patient safety and fortifying healthcare organizations against potential legal ramifications.

To explore this critical subject in more detail, read the full blog post here or listen to the on-demand webinar, "Review of HHS' Healthcare and Public Health (HPH) Cybersecurity Performance Goals," provided to our CloudWave Cybersecurity Insider Program members.

DISCLAIMER

The author is not a licensed attorney, and CloudWave is not a law firm. The thoughts represented here represent our opinions. Please discuss any specific recommendations or tactics with your legal counsel.

FROM THE FIELD: HEALTHCARE CYBERSECURITY IN ACTION

archcare Senior Life

Learn how ArchCare, the continuing care community of the Archdiocese of New York, uncovered the benefits of a robust cybersecurity tabletop simulation.

Even though they had done the right things to comply with regulations and best practices, ArchCare was concerned that they didn't know how to respond if the organization fell victim to a cyberattack. CloudWave delivered a series of tabletop simulations to place the IT and Executive teams in a real-feel cybersecurity situation. The tabletop simulation uncovered that ArchCare's incident response plan needed modifications, such as better defining communication protocols and explicitly identifying the backup person. During the cyberattack, the team also learned a process by identifying 'what is known' and 'what is not known,' which helped them reach faster decisions. Read the case study.

Emanate Health®

Learn how Emanate Health, a nonprofit healthcare provider in California's San Gabriel Valley, adopted CloudWave Cloud Hosting (an Infrastructure-as-a-Service solution) to enhance EHR security and safeguard patient care.

When Emanate Health's on-premises data center experienced a cybersecurity event, disaster was declared. At the time of the incident, the hospital was self-hosting its MEDITECH EHR. Following its recovery, Emanate Health turned to CloudWave Cloud Hosting to provide peace of mind and assurance that patient care would continue in the event of another cybersecurity event. Read the case study.

KEY TAKEAWAYS

Here are the essential points to keep in mind:

Cybersecurity is a "threat to life" in healthcare

Cyberattacks can have devastating consequences compromising patient care and safety. The FBI and DOJ now categorize hospital cyberattacks as "threat to life" crimes. This shifts the responsibility from protecting data to protecting lives; patient care must be prioritized first and foremost in any response effort.

The 72-hour compliance clock

Proposed regulations may shorten breach notification windows from 60 days to just 72 hours. Hospitals must move from passive monitoring to rapid, automated detection to meet these new timelines.

Proactive planning is crucial

Developing a comprehensive cybersecurity strategy and conducting regular risk assessments, training, and education can help prevent cyberattacks and minimize their impact.

Culture plays a critical role

Fostering a culture of cybersecurity awareness among IT and clinical staff, including leadership, is essential for effective cybersecurity.

Cybersecurity is an ongoing process

Staying up to date with the latest threats, technologies, and best practices is critical to maintaining a strong cybersecurity posture.

Resources and funding are available

The $50 billion Rural Health Transformation Program and other federal and state initiatives offer unprecedented opportunities for rural hospitals to strengthen their cybersecurity defenses. However, some programs require a funding-ready roadmap. Hospitals that conduct HIPAA security risk assessments and document infrastructure needs now will be first in line for state allocations.

Hospitals can further leverage the resources available in this guide and prepare now to take advantage of funding opportunities.

CONTACT US TO LEARN MORE →

REFERENCES

1. NRHA, Strengthening cybersecurity for patient care and data protection, April 24, 2025
2. CNN, America's rural hospitals keep getting attacked by cybercriminals, June 10, 2024
3. University of Minnesota School of Public Health, Rural hospitals may be more vulnerable to ransomware attacks, August 28, 2024
4. Healthcare Dive, Nearly 70% of healthcare organizations hit by cyberattacks report patient care disruptions: survey, October 8, 2024
5. Healthcare Dive, Nearly 70% of healthcare organizations hit by cyberattacks report patient care disruptions: survey, October 8, 2024
6. IBM, Cost of a Data Breach Report, 2025
7. MedCity News, Most Healthcare Organizations Have Paid $500K or More in Ransom Post-Cyberattack, Report Says, October 4, 2024
8. Microsoft, The Rural Hospital Cybersecurity Landscape, 2025
9. Microsoft, The Rural Hospital Cybersecurity Landscape, 2025
10. Chartis, 2025 Rural Health State of the State, February 10, 2025
11. Center for Healthcare Quality and Payment Reform, Rural Hospitals at Risk of Closing, December 2025
12. The 405 (d) Post, Rural Health and Cybersecurity
13. Journal of Rural Health, What happens to rural hospitals during a ransomware attack? Evidence from Medicare data, September 2024
14. Journal of Rural Health, How Do Ransomware Attacks Impact Rural Hospitals?, 2024
15. University of Minnesota Rural Health Research Center, Understanding the Rise of Ransomware Attacks on Rural Hospitals, June 2024
16. Journal of Rural Health, What happens to rural hospitals during a ransomware attack? Evidence from Medicare data, September 2024
17. Chartis, 2025 Rural Health State of the State, February 10, 2025
18. HIMSS, 2023 HIMSS Healthcare Cybersecurity Survey
19. Association of Health Care Journalists Report, How Medicaid Cuts Could Worsen Cybersecurity at Rural Hospitals, August 13, 2025
20. IBM, Cost of a Data Breach Report, 2025

100 Crowley Drive, Marlborough, MA 01752 877-991-1991 **gocloudwave.com**

CloudWave