



From Underserved to Audit-Ready: A Rural Health System's Cyber Transformation

Across the country, rural hospitals are under pressure.

Financial strain, workforce shortages, and increasing regulatory demands have pushed many to the brink—leading to dozens of closures and leaving entire regions without ready access to care. At the same time, these hospitals face the same cybersecurity risks as major health systems: ransomware attacks, third-party breaches, and evolving HIPAA enforcement from the Office for Civil Rights.

White River Health System, a nonprofit integrated delivery network serving 10 counties in north central Arkansas, knows this tension firsthand. With just under 200 licensed beds, a critical access hospital, 40+ clinics, and a small but dedicated IT team, they faced a clear challenge: how to build and maintain a strong cybersecurity program with limited resources and no room for error.

Instead of falling behind, White River took action. Since 2018, they've partnered with Clearwater to operationalize their risk management strategy — leveraging Clearwater's full IRM|Pro® software suite to gain visibility, prioritize remediation, document controls, and prepare for audit scrutiny. Today, they're not just meeting expectations — they've built a structured, risk-driven, and audit-ready program.

“We didn't really have good direction,” recalls Wesley Evans, IT Director. “We were just doing our own thing.”

Limited Resources, Expanding Risk

When White River first began evaluating its cybersecurity posture, the gaps were hard to ignore. Like many small health systems, they lacked a formalized program. Policies were inconsistent, documentation was scattered, and there was no clear path for managing risk across their network of hospitals, clinics, and systems.

It wasn't just about ensuring compliance with regulatory requirements — it was about managing cyber risk. Without a structured process in place, critical issues like excessive superuser access went unnoticed. The team knew they needed a more comprehensive approach, one that could help them both identify vulnerabilities and demonstrate measurable action.

But hiring a full-time consulting team wasn't feasible. With limited funding, a lean IT staff, and growing cybersecurity responsibilities, White River needed a solution that could flex with them — a system that would empower their internal team to drive progress without overextending their budget or their bandwidth.

They weren't looking for a quick fix. They were looking to build something sustainable.



A Platform Built for Progress

In 2018, White River partnered with Clearwater to bring structure, clarity, and forward momentum to their cybersecurity program. What began with a single solution grew into a full investment in Clearwater's IRM|Pro® platform — including modules for Risk Analysis, HIPAA Privacy and Security Rule assessment, and the 405(d) Health Industry Cybersecurity Practices (HICP) self-assessment tool.

The goal wasn't just to meet regulatory requirements — it was to build a living, adaptable system that could surface real risks and support continuous improvement.

To make that possible, White River's IT team embedded the platform into their weekly workflow.

"We dedicate time every Wednesday morning just to work in IRM Pro," said Evans. "It was tough to carve out at first, but it's become critical to our routine."

With guidance from Clearwater's on-demand expert support, they didn't have to go it alone. The team tapped into strategic help when needed, while taking full ownership of the program day to day. Over time, they developed deep familiarity with the tools, leveraging built-in frameworks and decision support to assess risk, track remediation, and document actions across their environment.

"The more I used it, the more I understood," said Systems Analyst Brandon Williams. "It helped me learn the environment, learn the risks, and get confident in what we're doing."

Turning Risk Visibility into Real Remediation

Since adopting Clearwater's platform, White River has transformed its cybersecurity program from a fragmented effort into a structured, risk-informed operation. Using the IRM|Analysis module, they've identified and addressed vulnerabilities that might have otherwise gone unnoticed — including a key finding involving excessive superuser access in a critical ambulatory application.

"We were able to go in, reduce that number, and bring it down to an acceptable risk level," said Evans. "That was a big win for us."

The 405(d) self-assessment tool also became an unexpected catalyst. Initially unfamiliar with the framework, the team quickly saw its value — not just as a checklist, but as a practical roadmap to policy development and operational hardening.

"We didn't even know we needed some of those policies," said Williams. "Now we've written them, implemented them, and are tracking them in IRM|Pro."

The impact has been felt across the organization. White River's cybersecurity efforts are now visible to the compliance committee, with clear documentation of what's been done, what's in progress, and how risks are being prioritized. That visibility has helped build trust with senior leadership — and boosted the team's confidence in their audit readiness.

"We can show what we're doing and what we've done," said Evans. "If OCR came knocking, I wouldn't say I'm excited — but I'd be prepared."



White River Health cyber-secure and on the move — ©White River Health



About White River Health

Located in Batesville, Arkansas, White River Health is dedicated to providing advanced healthcare in North Central Arkansas through inpatient and outpatient services as well as community outreach. With two hospital campuses, one in Batesville and one in Mountain View plus outpatient care centers and clinic offices throughout the region, WRH offers quality patient care and a healing environment—all right here at home.

About Clearwater

Clearwater helps organizations across the healthcare ecosystem move to a more secure, compliant, and resilient state so they can achieve their mission. The company provides a deep pool of experts across a broad range of cybersecurity, privacy, and compliance domains, purpose-built software that enables efficient identification and management of cybersecurity and compliance risks, and a tech-enabled, 24x7x365 Security Operations Center with managed threat detection and response capabilities.



Learn More

Whether you need help with risk analysis, responding to OCR, or a comprehensive approach to your cybersecurity and compliance program, we can help.

Guidance for Peers: Start Small, Stay Consistent, Use the Right Tools

For other small or rural hospitals facing similar challenges, the team at White River has a clear message: cybersecurity doesn't require a massive team or endless budget — but it does require commitment, consistency, and the right foundation.

“Don't ignore cybersecurity,” Evans advised. “Even if you're understaffed or underfunded, carve out time. Give it an hour a week if that's all you can give — but give it some time, every week.”

That deliberate, structured effort has been the difference for White River. With a platform that guides them through risk analysis, policy tracking, and remediation, they've been able to take real steps toward reducing vulnerabilities and demonstrating compliance.

And they're not doing it in isolation. Clearwater's built-in tools, frameworks, and strategic support help ensure they're staying aligned with industry expectations while tailoring the process to their specific environment.

“Clearwater helped us reach our goals,” said Evans. “We didn't just get software — we got a way to document, prioritize, and show our progress. And that's something we'd recommend to anyone.”

Built to Last: A Program That Supports the Mission

White River Health System isn't just managing risk — they're building long-term resilience. What began as an effort to bring order to their cybersecurity program has evolved into a structured, risk-driven strategy that supports ongoing improvement. Today, their team isn't reacting — they're leading: tracking risk over time, aligning to national frameworks like HIPAA and 405(d), and making informed decisions with confidence.

With Clearwater's IRM|Pro® platform at the center of that progress, White River has moved beyond reactive compliance to proactive risk management. Their work is documented, defensible, and visible to leadership — giving them the clarity they need to make smart decisions and stay ahead of evolving threats.

And they're not slowing down. Having recently renewed their IRM|Pro subscription for another five years, White River is doubling down on the tools and practices that have helped them strengthen security, improve oversight, and better protect the communities they serve.

“We value our relationship with Clearwater,” Evans said. “It's helped us build something we can stand behind.”