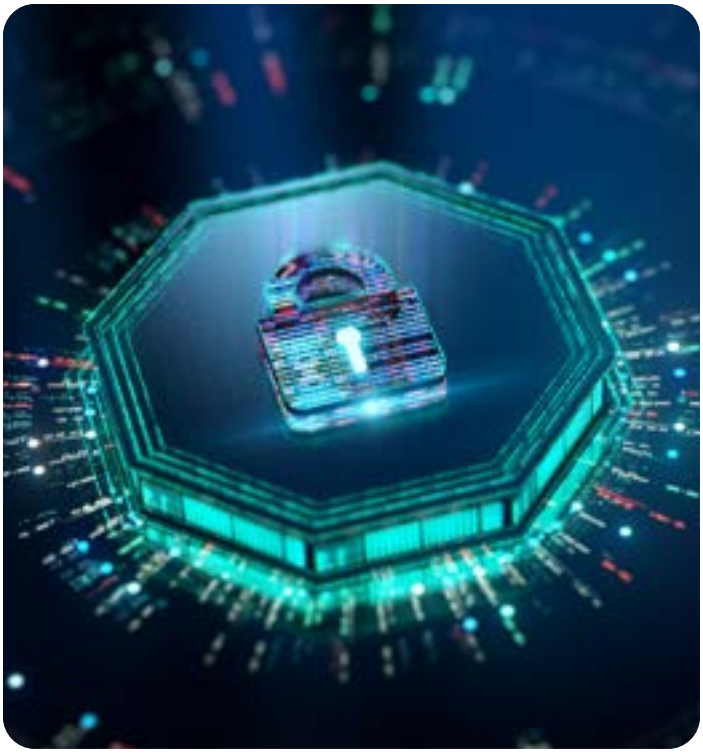
WHITE PAPER

Availity's Rapid Recovery

A Strategic Framework for Cybersecurity Resilience in Healthcare



Availity®



Executive Summary

Healthcare has become the most targeted sector for ransomware attacks—and the most vulnerable. With attackers now aiming at critical infrastructure like clearinghouses, the stakes have never been higher.

Despite this shift, many organizations still rely on outdated prevention-only strategies. But today, prevention alone is no longer enough. Cyberattacks are all but guaranteed. The difference between catastrophic disruption and business continuity lies in how fast an organization can recover.

Healthcare leaders must evolve their cybersecurity playbooks and demand more from vendors, including shorter recovery timelines, validated contingency plans, and real-world testing that ensures operational resilience—not just regulatory compliance.

In this white paper, we explore:

- Why prevention-only strategies fail in today's threat environment.
- How recovery speed is now a core business metric.
- What questions to ask vendors to assess their true resilience.
- How Availity's Rapid Recovery sets a new benchmark with independently validated five-day recovery time.

Introduction:
The Healthcare Cyber Crisis Has Arrived

In 2024, more than 276 million health records were exposed, making it the worst on record for breaches. This was an increase of 64 percent from the previous year, according to the Department of Health & Human Services (HHS) Office for Civil Rights (OCR). The exposed records represented nearly 81 percent of the U.S. population.

Most concerning was the February 2024 cyberattack on one of the nation's largest clearinghouses, which halted payment and eligibility transactions across the country, paralyzing providers, delaying care, and triggering billions in losses.

Healthcare is now the top target for ransomware attackers, surpassing financial services, government, and utilities. But while attackers evolve, many organizations remain stuck in a prevention-only mindset—hoping better firewalls and stricter access controls will stop the next breach. That mindset is dangerously outdated.

Since **cyberattacks are inevitable**, the true differentiator is **how fast you can recover**.

Healthcare Cyberattacks: The Numbers Behind the Crisis

276M	**A record-breaking 276 million records breached in 2024**
$14B	**$14 billion in damages from ransomware attacks in one year**
27 Day	**27 days average downtime per ransomware incident**
278% ⇧	**278% increase in healthcare ransomware attacks since 2019**
# 1 Target	**Healthcare faces more ransomware than any other critical sector**

© 2025 Availity, LLC AV340-0525

Prevention Isn't Protection Anymore

The problem with traditional prevention and recovery plans is they are ill-equipped to handle the data breaches of today.

Too many healthcare organizations still believe strong firewalls and compliance checkboxes are enough to protect them from modern threats. But the most damaging cyberattacks of the past two years proved one thing, prevention alone can fail.

And when prevention fails, outdated recovery models leave organizations stranded. Most technology vendors still offer basic disaster recovery plans built around legacy assumptions such as: downtime will be short, backups will be sufficient, and operations can resume quickly.

These assumptions are woefully outdated. Which leaves one thing abundantly clear: prevention has become table stakes. Healthcare must now plan not only for *how to stop an attack*, but also for *how to survive one*.



When Recovery Fails, the Healthcare System Fails

When a breach occurs, the true cost goes far beyond IT.

From missed appointments to unpaid claims and from delayed prescriptions to damaged reputations, cyberattacks impact operations, finance, and services—for patients, providers, and payers alike.

The traditional recovery process itself can be slow and painful:

1. Systems go offline—often for weeks.
2. Forensic teams must search for vulnerabilities.
3. Data integrity is verified and restored.
4. New environments are tested and rebuilt.
5. Third-party attestations are required before go-live.

That's assuming you have a recovery plan at all. Most organizations rely on a third-party software vendor. If your vendor's plan is weak, your operations fail too.

If Your Vendor Can't Recover Fast, You Can't Either

In healthcare, technology vendors aren't just service providers—they're critical infrastructure. When clearinghouses, electronic health records (EHRs), or claims platforms go down, entire regions grind to a halt.

Since most healthcare vendors are still focused on prevention, when a breach occurs, they lack a true recovery plan—making themselves vulnerable to a crippling cyberattack.

That's no longer acceptable.

Healthcare organizations must demand more from every vendor. The new question isn't just "How secure are you?" but "How fast can you bring us back online after an attack?"

The most resilient industries—banking, defense, and telecommunications—don't just plan to prevent breaches. They engineer for recovery. Healthcare must follow suit.

That means ensuring:

- Independent validation of recovery protocols.
- Real-world attack simulations, not just tabletop exercises.
- Redundant, immutable backups that can't be encrypted or erased.
- Defined, contractually backed recovery timelines.

Anything less isn't resilience—it's a liability.

© 2025 Availity, LLC AV340-0525

Vendor Evaluation Guide: 5 Questions Every Vendor Must Answer Before You Sign

In the wake of healthcare's most disruptive cyberattacks, vendor vetting can't focus only on features or compliance certifications. You need to know: **Can this partner get my organization back online—fast?**

1. **What is your recovery time after a cyberattack?** If they can't commit to a specific timeline, they're not ready.
2. **How do you ensure your backups are secure and immutable?** Ask if they use air-gapped or physically isolated systems that ransomware can't touch.
3. **Do you run real breach simulations—or just tabletop exercises?** Practice makes you prepared. Look for vendors who stress-test their recovery plans in live scenarios.
4. **Can you maintain communication during a total outage?** Clear, redundant communications are critical to coordinating recovery across stakeholders.
5. **Do you offer third-party validation of your recovery capabilities?** Independent audits ensure you're not just taking their word for it.

Some vendors and clearinghouses do the bare minimum, following only what's required to stay compliant. For instance, if vendors only perform breach assessments after an incident or annually—or never—that's unacceptable.

It's important to find a vendor who does more than the minimum by providing protection, detection, and recovery. When considering potential technology vendors, pay attention to the following red flags:

- Reliance on compliance certifications without real recovery capabilities, because compliance alone is proving inadequate.
- Slow recovery timelines, which mean delays in care and lost revenue.
- Lack of real-world testing—leaving organizations vulnerable to significant disruption.
- No independent validation, which ensures necessary protection and verifies recovery plans.

In an industry where downtime costs millions—and impacts lives—your vendor's resilience is your resilience. It's more important than ever to choose wisely.

Conclusion – The New Cybersecurity Playbook

The old cybersecurity strategy—build stronger walls and hope they hold—is no longer viable.

Instead, a three-pronged approach of prevention, detection, and recovery must become the standard for the industry. Traditional recovery models are reactive and take weeks to recover if not longer. But a proactive approach accelerates recovery and gives organizations more protection—helping thwart attacks before they happen.

With cyberattacks increasingly inevitable, the only question is how prepared you are to recover *when*—not *if*—your systems go down. That means shifting the playbook:

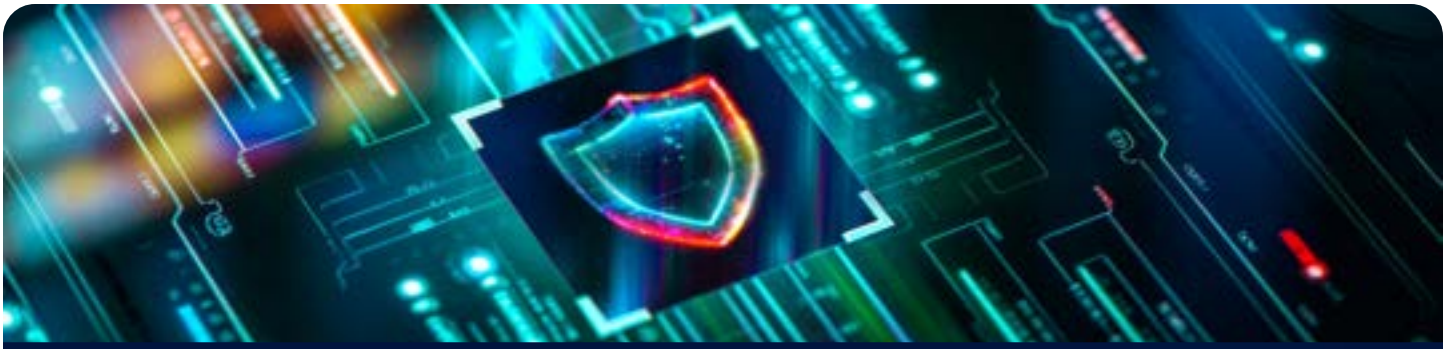
- From **prevention-only** to **prevention plus rapid recovery.**
- From **vendor trust** to **vendor verification.**
- From **reactive responses** to **resilience by design.**

Your technology vendors aren't just vendors, they're digital lifelines. If they fail to recover, your organization fails too.

With recovery time increasingly critical to operations, choosing a third-party vendor takes on even more importance. Vendors who provide cybersecurity to organizations and their partner vendors should consistently and thoroughly test for resilience against cyberattacks.

That's why Availity® created **Rapid Recovery**—a new standard for business continuity in healthcare. With a five-day recovery guarantee, independent validation, and hardened infrastructure inspired by military and financial systems, Availity is leading the way in making recovery speed a measurable, contractual promise—not an aspiration.

© 2025 Availity, LLC AV340-0525



5 Takeaways from the 2024 Healthcare Data Breach

The 2024 healthcare cyber attack involving Change Healthcare was a wake-up call, exposing critical vulnerabilities in handling sensitive data. Simply put, it was the most significant and consequential cyberattack in the history of U.S. health care to date. Just over one year later, the industry continues to learn valuable lessons to bolster its defenses and improve response strategies.

1. **Cybersecurity is an Organization-Wide Priority**
   Cybersecurity is no longer just an IT issue. Leadership must drive a culture of security, ensuring that employees at all levels are trained to recognize and mitigate threats. Executive support and security awareness programs are crucial in strengthening defenses.

2. **Downtime is More Costly Than Anticipated**
   The Change Healthcare attack demonstrated that disruptions extend far beyond initial estimates, with financial repercussions including legal fees, system repairs, and regulatory fines. The average cost of a breach is $11 million according to research conducted by the Ponemon Institute.

3. **Compliance is the Baseline, Not the Goal**
   To keep pace with evolving threats, healthcare organizations should proactively implement best practices to enhance security beyond minimum compliance requirements. Certifications like HITRUST (formerly the Health Information Trust Alliance) and EHNAC (Electronic Healthcare Network Accreditation Commission) accreditation are now essential.

4. **Communication is Critical in a Crisis**
   Clear, transparent communication is vital during cyber incidents. Quick stakeholder notifications and cross-industry collaboration help contain threats and mitigate damage, reinforcing the importance of information-sharing among organizations and government agencies.

5. **Recovery Requires Proactive Planning**
   Organizations must prepare comprehensive response strategies, including security assessments, penetration testing, and adaptive recovery protocols. A robust cyber defense should balance both proactive and reactive measures to minimize future risks. By learning from past attacks, the healthcare industry can build stronger defenses, ensuring better resilience against future threats.



Don't Let Disruptions Define You.

Recovery speed is now a competitive advantage—and a leadership imperative. Find out how Availity's Rapid Recovery can help you stay resilient, protect patients, and maintain trust—even in the face of a major cyberattack.

Visit Marketing.availity.com/RapidRecovery to learn more.

© 2025 Availity, LLC AV340-0525

Sources:

- Alder, Steve. "Healthcare Experiences More Third-Party Data Breaches Than Any Other Sector," HIPAA Journal, March 4, 2024. https://www.hipaajournal.com/healthcare-highest-third-party-breaches
- Eddy, Nathan. "Ransomware Downtime Costs U.S. Healthcare Organizations $1.9M Daily." Healthcare IT News, 31 Dec. 2024, www.healthcareitnews.com/news/ransomware-downtime-costs-us-healthcare-organizations-19m-daily.
- ISC2. (2023). How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce 2023. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf
- By Brian Shimabukuro and Siriam Sekar with Angela Botner and Rut Patel. Tech resilience for healthcare providers: Inaction has a heavy toll. McKinsey, February 18, 2025. https://www.mckinsey.com/industries/healthcare/our-insights/tech-resilience-for-healthcare-providers-inaction-has-a-heavy-toll
- Alder, Steve. "Change Healthcare Responding to Cyberattack." HIPAA Journal, 25 Jan. 2025. www.hipaajournal.com/change-healthcare-responding-to-cyberattack/.
- Cost of a Data Breach Report 2024. IBM, July 30, 2024. https://www.ibm.com/reports/data-breach
- What are the penalties for HIPAA violations? https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/
- Is it Time for the Healthcare Industry to Re-examine Cybersecurity Preparedness in the Face of Undprecendented Risk. October 8, 2024. https://www.healthcareittoday.com/2024/10/08/it-is-time-for-the-healthcare-industry-to-reexamine-cybersecurity-preparedness-in-the-face-of-unprecedented-risk/
- Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double. FBI, February 28, 2024. https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf#:~:text=Worldwide%20ransomware%20attacks%20against%20the%20healthcare%20sector,victims%20in%202023%20versus%20113%20in%202022.