From Cybersecurity Crisis to Continuity: Availity® 5-Day Rapid Recovery Framework

Healthcare has become one of the most targeted and vulnerable sectors for ransomware attacks. With cybercriminals now aiming at critical infrastructure like clearinghouses, the stakes for health plans and providers have never been higher.

These attacks don't just compromise data—they threaten the very connections that keep healthcare operations running.

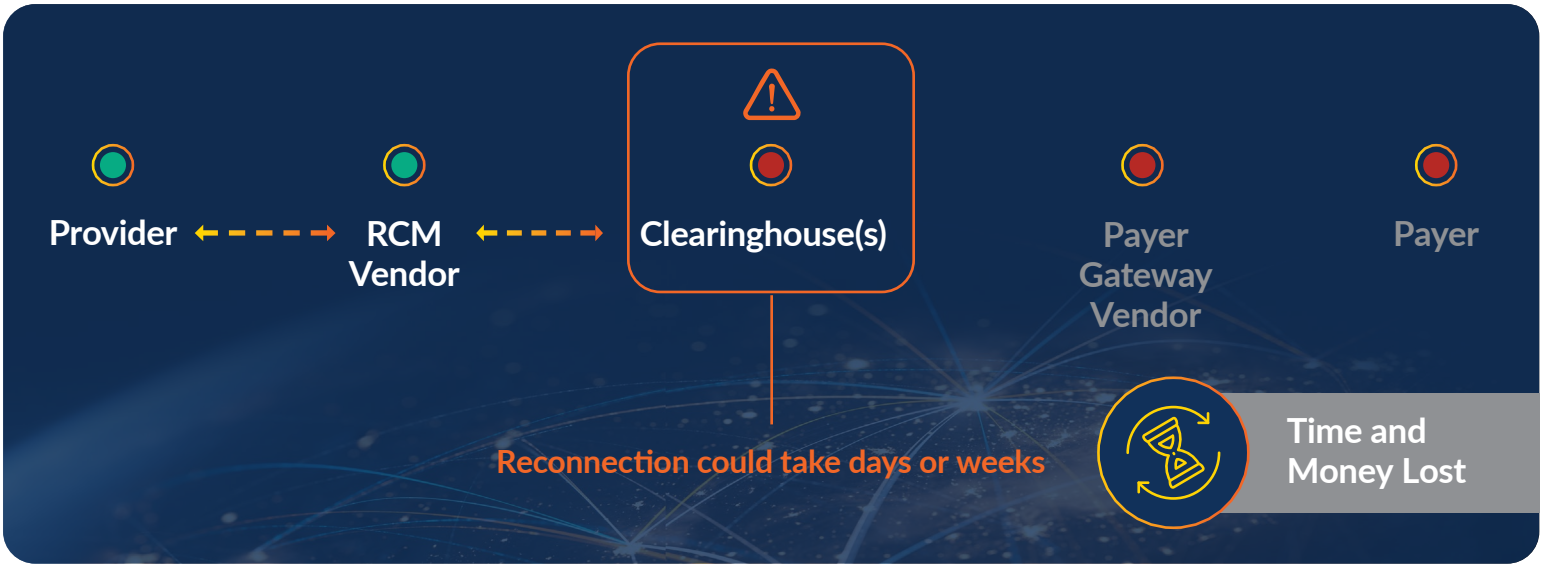
Connectivity across the healthcare ecosystem is both complex and essential. The seamless exchange of transactions depends on a vast network of interconnected systems.

Disrupt just one link in this chain, and payment flows halt putting financial stability, operational efficiency, and ultimately patient care at serious risk.

Each healthcare transaction relies on a chain of systems working in unison

Behind every healthcare interaction lies a vast, invisible web of systems and connections working seamlessly to keep vital health plan and provider operations flowing, from verifying coverage to processing payments.

A single compromised link halts transaction flow for everyone connected—disrupting payments, operations, and care delivery.



When a cyberattack hits any link in the chain, healthcare transactions immediately stop. An impacted organization needs to investigate, remove threats, and rebuild systems—a process that can take significant time.

During the downtime, claims backlog, payment delays, and stalled patient care decisions create a ripple effect.

Billing issues tighten revenue cycles, and admin teams work overtime handling manual processes and a surge in patient questions, disrupting day-to-day operations.

Even after systems are back online, recovery isn't simply about restoring technology

When any of these systems are compromised, it can't simply reconnect to its partners once systems are back online.

Healthcare networks require independent, expert validation to ensure all threats have been fully removed. Until that verification happens, connections remain blocked.

If your technology vendor can't recover fast, neither can you.

System failures due to cyberattacks and lengthy recovery times are costing healthcare organizations millions of dollars in manual processes, claim backlogs, and emergency staffing. The financial and reputational damage can be devastating. It doesn't have to be this way.

Availity's Rapid Recovery program can help you stay resilient, protect patients, and maintain trust—even in the face of a major cyberattack.

Availity's Rapid Recovery: Setting a New Standard for Business Continuity in Healthcare

Traditional recovery models are reactive and take weeks to recover if not longer. That's why Availity developed the Rapid Recovery program, to raise the bar for business continuity in healthcare with a five-day recovery framework, third-party validation, and a fortified infrastructure modeled after federal and financial standards.

Here's how it works:

1. Pre-Validated System Backups

Availity creates secure, pre-validated system backups on a regular basis to avoid scrambling to assess compromised systems after an attack. The system backups include not just the data we house, but also the configurations that tell us what to do with that data and the code behind our products.

2. Third-Party Security Validation

One of the biggest challenges in cyber recovery is ensuring that attackers haven't left behind hidden threats. Our system backups are pre-cleared by Mandiant, one of the top cybersecurity firms in the industry. This independent attestation eliminates reliance on trust alone because it's verified.

3. Immutable, Air-Gapped Storage

The system backup is stored in a completely isolated, secure environment—like a vault that no one can alter or access without strict controls. It's physically and digitally separated from other networks to prevent tampering or infection, even from inside threats.

4. Threat Detection & Additional Scanning

If a cyberattack is suspected, the backup is pulled from the vault and rescanned for safety by Mandiant to ensure it's safe from intruders.

5. Rapid Recovery & Reconnection

These validated backups are restored in a new environment, further isolated from contamination. Through these steps, Availity enables system restoration and partner reconnection within five days following ransomware attack, significantly reducing disruption.

Learn More

Visit **Marketing.Availity.com/RapidRecovery** to learn more.

Availity®