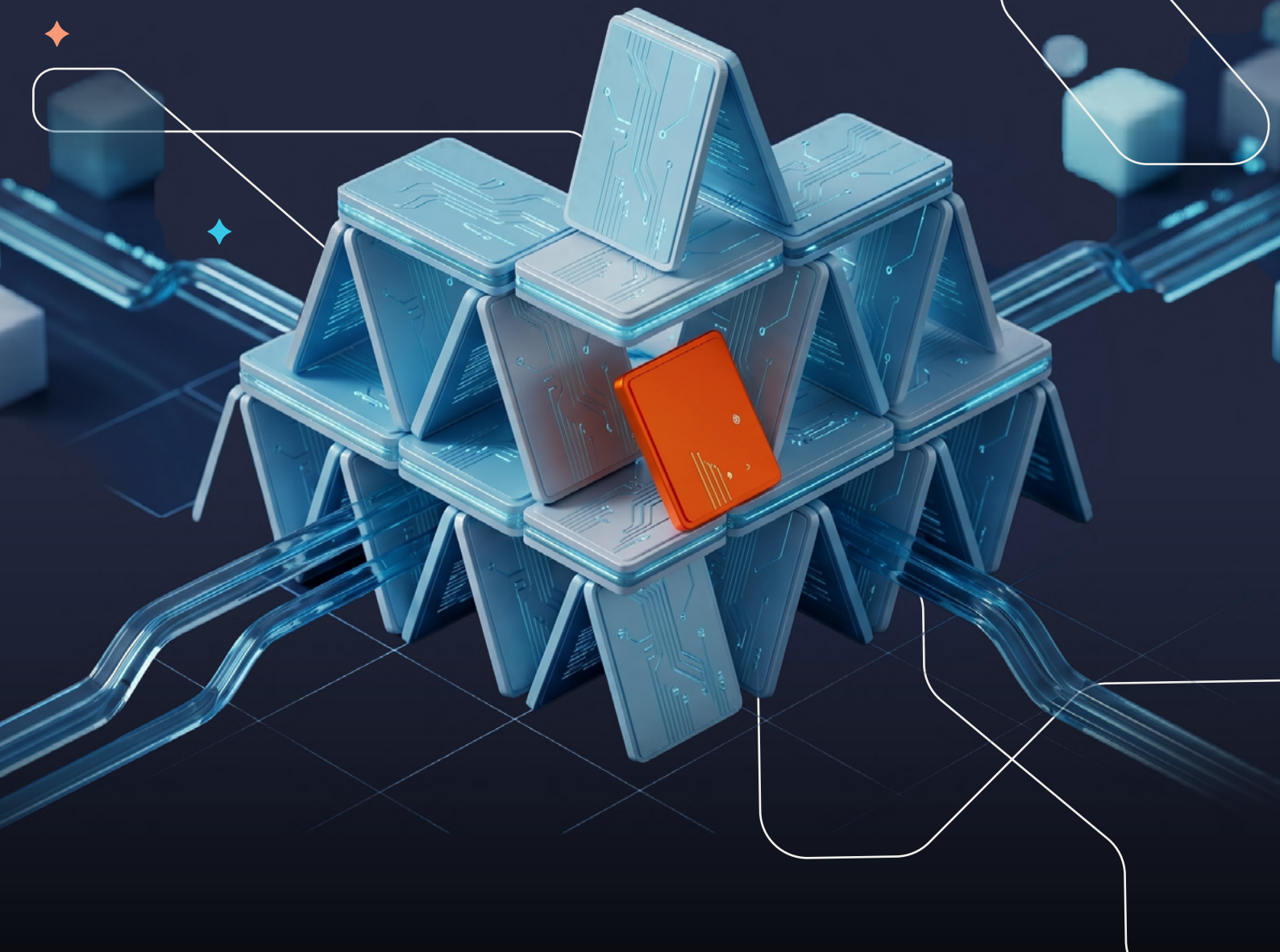
TEAM8™ 7wire

AI and the Healthcare House of Cards: Will it Break or Build Cyber Resilience?

By Assaf Mischari, Managing Partner, Team8
Dror Grof, Partner, Team8
Lee Shapiro, Managing Partner, 7Wire



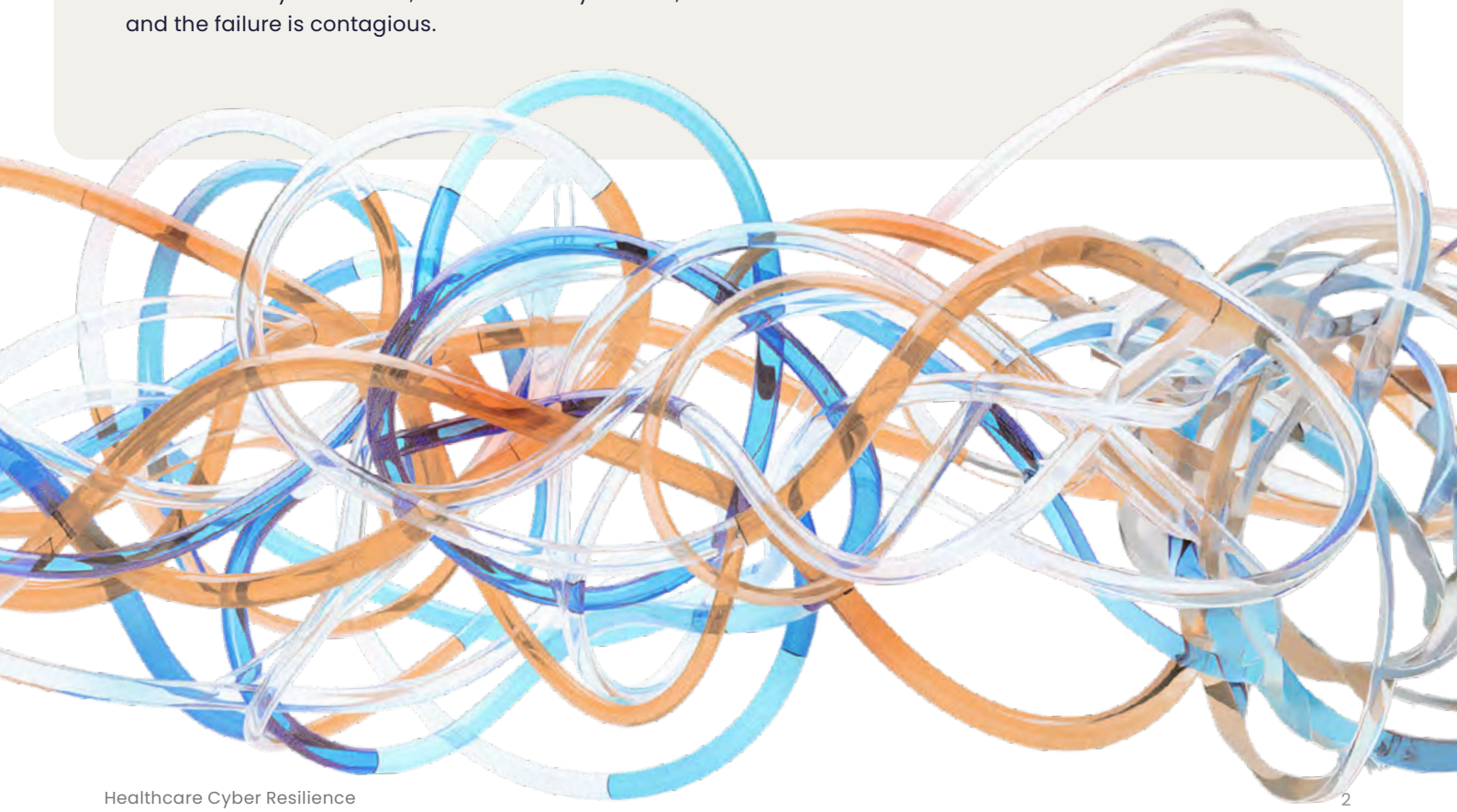
Forward

American healthcare is at major risk of becoming structurally unsustainable. Not because care practices are failing, but because the infrastructure beneath care has become so interdependent that a single disruption can trigger system wide fallouts. Healthcare systems currently depend on a dense web of invisible intermediaries: clearinghouses, identity providers, scheduling platforms, pharmacy networks, and revenue cycle engines, just to name a few. These dependencies were optimized for efficiency and reliability on constant availability, leaving many systems ill equipped to degrade safely under stress, outages, or disruption. And to make matters worse, if even one critical link in a healthcare system goes down, the effects rarely stay contained: they cascade across claims, prescriptions, labs, and frontline workflows– with patients and clinicians absorbing the consequences.

This is the defining fragility of modern healthcare: interdependence without practiced fallback. In theory, critical workflows in healthcare and hospitals can revert to manual processes during downtime. In reality, those pathways are rarely rehearsed, rarely staffed, and often no longer viable at scale. The system works, until it suddenly doesn't, and the failure is contagious.

Enter AI. As much as AI is advancing the healthcare system at unprecedented speed, it is paradoxically the compounding factor that makes the system's current interdependence structurally unsustainable as each new tool adds dependencies and architectural complexity. As artificial intelligence automation absorbs more clinical and administrative work, it quietly erodes what healthcare needs to survive disruption: practiced human skills, staffing capacity above the automated baseline, and clear, tested contingency routes.

Still, the upside is too large to ignore, with the status quo failing patients and clinicians through delays, shortages, and preventable administrative drag. Healthcare needs these advances. AI is reducing burden, expanding access, and enabling care that was not possible before. But healthcare cannot afford an interdependent backbone that becomes structurally unstable the moment a single component breaks. The question is no longer whether AI will be adopted. It is whether resilience can be rebuilt fast enough to keep the system safe as automation deepens.



What breaks when the system breaks? Change Healthcare was not a surprise, it was a symptom of flawed and systemic interdependence

In February 2024, a ransomware attack on Change Healthcare froze the pipes of American healthcare. It wasn't a particularly sophisticated cyberattack: one portal, no multi-factor authentication, one password.

Within hours, the central nervous system of American healthcare went dark. Sensitive medical data belonging to roughly 190 million Americans was compromised.

Healthcare Cyberattack Impact

190 million
Americans' Sensitive Medical Data Compromised
Central nervous system of healthcare went dark.

$2 trillion
Medical Claims Froze in Processing
Over 900,000 physicians affected.

900,000
Physicians Unable to Submit Insurance Claims
5,500 hospitals and 600 laboratories also affected.

67,000
Pharmacies Could Not Verify Patient Coverage
33,000 pharmacies unable to submit claims.

TEAM8

Many of those harmed by the outage did not even know Change Healthcare existed. As Fortune noted, one physical therapy practice owner "had no idea his billing company even used Change's technology."
Dr. Jesse Ehrenfeld, ex-president of the American Medical Association, put it plainly: "Most physicians had no idea that Change Healthcare touches more than a third of all health care transactions in the nation."

This is exactly what makes the incident so dangerous at a systems level: critical infrastructure became a single point of failure while remaining invisible to the people relying on it every day.
The breach disrupted operations for weeks. UnitedHealth Group, Change Healthcare's parent company, later disclosed paying approximately $22 million in ransom. Even after payment, restoration took weeks, reflecting the assumption that Change would always remain operational. There was no contingency plan, no alternate pathways, no manual processes anyone remembered how to use.

> The most surprising is also the most common, human error."

Brian Griffin
NWM CISO

This wasn't healthcare's first major crisis. But it exposed a reality we can no longer ignore: American healthcare operates on a digital house of cards so fragile that a single failure can collapse the entire system. When one card is pulled, claims stop, care is delayed, and pharmacies disconnect.

> **The consequences are not abstract: multiple studies have found that cyber incidents in hospitals are associated with a relative increase in inpatient mortality of more than 20%.**

Change Healthcare Wasn't The Only Disaster

Universal Health Services (September 2020): A ransomware attack attributed to Ryuk forced UHS to take IT systems offline across its 250+ U.S. facilities. No access to patient histories. Lab systems down. Pharmacy systems offline. Surgical schedules kept on whiteboards. The entire system was thrown back technologically by half a century. Clinical systems were restored on a staggered basis over several weeks, with UHS disclosing an estimated $67 million financial impact, driven primarily by lost operating income related to decreased patient volumes, billing delays, and recovery costs. Despite heavy cybersecurity investment and disaster recovery capabilities, the incident exposed a deeper truth: centralized digital dependencies had become single points of systemic failure.

Scripps Health (May 2021): A ransomware attack encrypted critical systems, disrupting access to electronic health records, imaging, and scheduling. Despite prior investments in redundancy and disaster recovery, Scripps was forced to take large portions of its infrastructure offline. The incident caused roughly 30,000 appointment cancellations and ambulance diversions for weeks. Backups were intact but couldn't be restored quickly enough while recovery required extensive system validation and rebuilding authentication infrastructure, taking over a month. Scripps later reported approximately $112.7 million in losses.

While security gaps in healthcare are real, closing them does not solve the underlying problem. What healthcare faces is a resilience engineering failure that is merely illustrated by security events.

> **The industry keeps adding better locks to the doors, but when someone gets inside, the entire house collapses. Security may be the catalyst, but the catastrophe lies in systems that cannot function when even a single component fails.**

Interconnected vs. Interdependent: Where Healthcare Systems Fall

Silicon Valley loves to talk about interconnected ecosystems. Healthcare built something different: interdependent systems.

In an interconnected system, there are multiple routes between points. If one route goes down, traffic reroutes and the system degrades predictably. The Internet works this way. A single component failure affects only that component. In an interdependent system, failure is contagious. Each step depends on the previous step, with few alternatives and few practiced workarounds. When one link fails, the workflow behind it fails with it–not because redundancy is impossible, but because redundancy was never treated as a design requirement.

Other industries design for fallback as a default: retailers route payments from Visa to Mastercard or to cash; airlines shift to backup systems or manual card processing; power grids reroute load and isolate failures so a single breakdown does not break the whole system down. In healthcare, when a central clearing path fails, billing halts, prescriptions stall, and procedures get canceled, because there is often no equivalent alternate route. One integration, one clearing path, one identity provider, one primary interface, and a fallback system that is entirely manual and unrehearsed.

Data interoperability issues further compound the complexity of the problem. Healthcare data often moves through narrow, vendor specific interfaces and centralized exchange layers, not through resilient, redundant pathways. When a major system fails, teams cannot simply switch to an alternate tool and keep operating, because the patient context, clinical history, orders, and administrative state do not transfer cleanly. Interoperability was treated as connectivity, not as a resilience layer, with outages having the potential to create data blind spots that are not easily fixed.

These fallshort approaches were survivable historically, when systems mainly digitized existing work and teams retained the skills to revert under pressure. AI is changing the operating conditions, adding layers of automation while simultaneously removing human touchpoints. What's left is a reality where staff don't know how to operate without multiple layers of automation and continuity of patient context and data.

Lessons in Systemic Resilience from Other Industries

Other industries learned this lesson the hard way. After 9/11 exposed how a single catastrophic failure could destabilize the entire financial system, financial infrastructure was redesigned to withstand worst-case disruption. Visa conducts regular "disaster days," intentionally breaking systems to test recovery. Aviation built triple redundancy into critical systems. Netflix uses Chaos Engineering to randomly disable servers in production. These industries don't eliminate failure, they make failure non-catastrophic by design. Healthcare, by contrast, has largely assumed failures will be rare and work can revert to manual when needed.

That assumption is becoming less true every year, not only because systems are more connected, but because automation has been steadily removing the human capacity that manual mode requires. As AI and workflow automation expand throughput, organizations practice the fallback path less, specialists lose fluency in the underlying tasks, and staffing levels are recalibrated around the automated baseline.

When an outage hits, teams are asked to do two impossible things at once, absorb higher volumes manually and do it with fewer people who remember how.

> An unfortunate reality in healthcare is that the complexity and impact of prolonged system downtimes are so daunting that many systems default to prevention and prayer rather than practice; a choice that usually works, until it doesn't.'"

Hal Baker
Former CIO
WellSpan Well at Work

AI Is The Forcing Function That Will Make This Model Unsustainable

Healthcare is currently outpacing every other industry in the US in AI adoption, with a 63% full-deployment rate compared to the 50% cross-industry average, according to NVIDIA's 2025 State of AI in Healthcare report.

Hospitals are leading this adoption with 71% of US facilities now actively using predictive AI tools for clinical and operational decisions. As the AI tools and technology pile on fast, workflows are becoming increasingly dependent on them while the interdependencies grow. When even just one fails, the results are even more catastrophic.

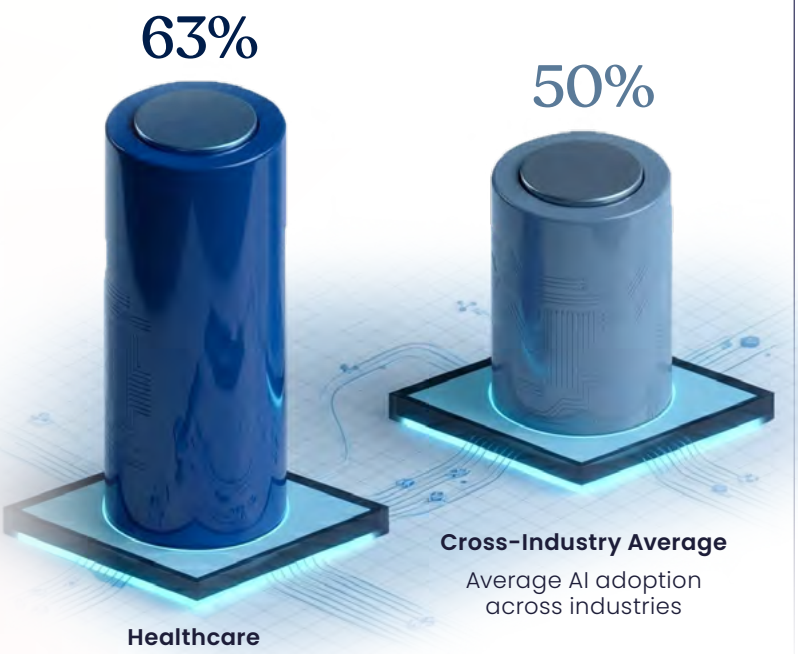
AI is being urgently onboarded to aid the current staffing and revenue crisis of the healthcare systems, but along the way, it erodes resilience in three quiet ways:

1. As automation absorbs more of the work, skills degrade because critical tasks are practiced less
2. Capacity shrinks because staffing models get rebuilt around the assumption that the integrated technology will always be available
3. Complexity compounds exponentially as each AI layer multiplies risks

> Once AI absorbs the work, the skills and excess capacity behind the old model inevitably erode, making engineered fallback paths and redundancies the real requirement.

Assaf Mischari
Managing Director
TEAM8™

AI Adoption Rates in US Industries



Skills: Medical and Administrative Expertise Atrophies at AI Speed

The most dangerous skill erosion is the kind nobody notices until it's too late. When AI handles a task reliably for months or years, the humans who once performed it lose fluency, not because they forgot the theory, but because they stopped practicing.

Consider revenue cycle management. Successful RCM requires both scale and skill: coders navigating complex diagnosis hierarchies, billers understanding payer-specific rules, specialists untangling denied claims. In highly automated environments, these competencies have eroded to a point that is now insurmountable.

A revenue cycle team relying on automated claim submission, eligibility checks, and denial management cannot simply revert to paper and fax if systems go down. Employees who no longer practice the technical expertise cannot manually navigate coding lookups, payer phone trees, and reconciliation logic. The muscle memory is gone. The staff who remembered how things worked before automation have retired or moved on.

The same pattern plays out clinically. When a radiologist has relied on AI-assisted detection for years, their ability to catch subtle findings without assistance degrades - pattern recognition requires constant practice. Ambient documentation tools transcribe notes automatically; when they fail, clinicians discover their documentation skills have atrophied from disuse.

> **The cruel irony is that the tasks most worth automating (repetitive, high-volume, error-prone) are precisely the tasks requiring the most practice to perform manually. By automating them, we make fallback functionally impossible at healthcare's scale. This degradation of manual capability can extend far beyond the clinical staff. As Christian Lindmark, CTO of Stanford Healthcare, points out, the invisible IT infrastructure is highly susceptible: "We spend far more time rehearsing clinical downtime procedures than failures of AI-enabled operational workflows. The risk is that operational muscle memory gradually shifts from humans to systems."**

Capacity: Staffing Models Rebuilt Around Permanent Uptime

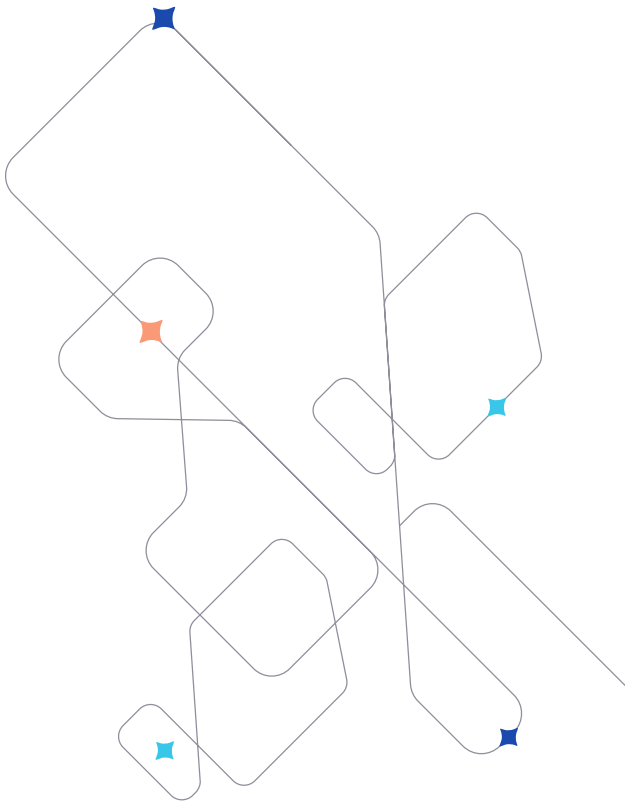
Skills atrophy is one problem. Capacity erosion is worse, because it's irreversible in the short term.

When AI increases throughput, organizations don't maintain old staffing levels as buffer, they reduce headcount. Rational at the organization level, but catastrophic at the system level. The slack that allowed manual operations during outages no longer exists.

Consider healthcare call centers. AI systems can push tens of thousands of appointment reminders, care gap prompts, and follow-up calls daily. Before automation, this required large teams. After automation, those teams have been reduced by half.

When that layer goes down, remaining staff cannot replicate it manually. A team of 20 cannot do work that requires 100. Patients don't get called. Appointments are missed. Revenue leaks.

Care management follows the same trajectory. AI tools now identify high-risk patients, prioritize outreach, and automate coordination that once required large teams.



Complexity: Each AI Layer Doesn't Just Add Risk, It Multiplies Risk

The third erosion mechanism is the most insidious: exponential complexity.

AI introduces different complexity. Each layer adds dependencies: data access, identity services, model hosting, vendor uptime. But more importantly, AI layers interact in ways that create emergent failure modes that no component-level analysis would predict.

Consider a hospital with ambient documentation, clinical decision support, automated coding, predictive analytics, and AI scheduling. When ambient documentation fails, it doesn't just affect notes. It affects clinical decision support, which depends on structured note data. It affects coding, which depends on documentation. It affects predictive models trained on data that assumed ambient documentation would be present. Failure cascades unpredictably.

This is multiplicative complexity. Three AI systems don't create three times the complexity, they create the complexity of each system plus every possible interaction. The observability problem compounds this. With AI, connections are often implicit, mediated by data flows and integration patterns not documented anywhere. When something breaks, teams don't know what else is affected until secondary failures appear. As Christian Lindmark observes, "In practice, outages often become the most honest system diagrams we have. Tabletop exercises help, but they rarely capture every dependency, especially when third-party vendors are involved." Relying on catastrophe as an architectural discovery tool is a gamble the healthcare system can no longer afford.

AI increases these stakes but also offers partial remedy. The same intelligence automating work can map workflows, trace dependencies, and make resilience visible. Observability must be a design requirement: continuous mapping of dependencies and planning fallback paths before the next failure tests them.

> **But AI integration is also a paradox: the same technology that intensifies risk can be used to map dependencies, surface hidden fragilities, and make resilience visible across organizations. That visibility is the first step toward designing for failure instead of assuming it won't happen.**

Each healthcare organization needs precise mapping of its personal processes, workflows, interdependencies, and unique vulnerabilities: one size fits all solutions will not work. A Team8 cybersecurity portfolio company, Nagomi, is a concrete example of what observability can look like in security. Nagomi connects to an organization's existing security tools and unifies data across assets, defenses, and threats, so teams can see where they are exposed, where controls fall short, and which issues create the most real world risk, then track remediation progress and report improvements over time. Applying this to healthcare, that same model would help organizations move from generalized understanding of the technologies they use, to specific guidance about where dependencies concentrate, which controls are actually effective, and which fixes reduce the risk of a cascading failure first.

> The same principle of using AI as the key to solving the complexities it creates applies beyond security. Platforms that integrate AI to unify fragmented clinical and administrative workflows can reduce systemic fragility by reducing the number of system to system transfers required, and making care context easier for providers and patients.

Lee Shapiro
Managing Director
7wire

Take Transcarent, a 7wireVentures backed health and care platform that brings together benefits navigation, clinical guidance, and on-demand care into a single AI assisted interface that its members enjoy interacting with. This kind of consolidation platform reduces friction for patients and limits the number of places a process can stall, with care routing handled in one coordinated flow instead of being handed off across disconnected vendors.

> **Even with incredible solutions, the resilience question does not change. When any single layer goes unavailable, are there alternate routes and downtime modes, and are those fallbacks designed and rehearsed rather than assumed?**

Why Now? The AI Inflection Point

This is the optimistic framing about AI in healthcare, and it ends as a warning. AI does not merely increase risk in healthcare systems; it changes the operating model in ways that make resilience a prerequisite, not an enhancement.

We are building a healthcare system that is smarter, faster, and more automated than ever before, yet paradoxically more brittle. By allowing skills to atrophy and assuming technology will always be available, we have created a single point of failure that no amount of cyber insurance can cover. Each AI workflow that replaces a human capability without a deliberate fallback plan quietly increases systemic fragility.

The choice is not between investing in resilience or investing in AI. The point is that AI forces the issue. If healthcare keeps stacking automation on top of brittle foundations, the next Change Healthcare disaster will not only freeze claims and prescriptions, it will take down the AI-enabled processes that organizations increasingly rely on for clinical and operational decisions.

> Our design philosophy is that AI should augment workflows and not become a single point of failure. Clinical workflows must still function safely even if AI disappears."

Christian Lindmark
CTO
Stanford HEALTH CARE

There is a path forward, and it does not require reverting back to manual processes and abandoning hope on a future with automated software or AI systems. It requires designing them differently: building observability into AI programs, maintaining human fluency in critical workflows, segmenting dependencies, and rehearsing fallback paths as rigorously as we rehearse clinical emergencies. Automation can strengthen healthcare, but only if resilience is engineered alongside it, not bolted on afterward.

The way healthcare integrates AI into its systems is the moment the house of cards either gets rebuilt on something sturdier, or it collapses under its own weight and patients absorb the consequences.

Part 2 of this article will provide the answer key: how to design observability into AI programs, how to build rehearsed fallback paths, and how to prevent skills and capacity from becoming your most expensive hidden risk.