Microdosing

Safety is Sexy in Healthcare B2B Sales

Why Risk, Not Upside, Decides Deals

Paul Schrimpf, Christine Arbesman

Microdosing delivers short, fact-driven reports that distill today's trending healthcare topics, and add fresh perspectives that are grounded in expert insights and credible data. For more information, as well as an audio version of this report, go to: **www.md-pod.com**

In healthcare B2B sales, the deal is often shaped before ROI is fully debated. It begins when a buyer asks a simpler question: what could go wrong?

Healthcare sales is methodical, slow, and process heavy. Health systems are not optimized for novelty or speed alone. They are optimized to avoid harm while maintaining continuity of care. Safety may not sound exciting, but for anyone selling into a hospital or large health system, it is often where deals gain or lose momentum.

Buyers are not primarily asking how much upside a solution creates. They are asking how much risk it introduces. That does not mean upside is irrelevant. It means upside is filtered through a risk lens.

In practice, that risk looks concrete:

- A system outage that delays care
- A workflow change that increases clinician error
- A cybersecurity incident that exposes patient data
- A technology rollout that destabilizes existing processes

These are not hypothetical concerns. Research on clinical technology disruptions and workflow shows that health systems have experienced these scenarios. Many carry the scars in the form of clinician frustration, public headlines, regulatory scrutiny, and real patient impact.

As Tampa General Hospital's Chief Transformation Officer, Peter Chang, said on Healthcare Rap, "As much as we want to say that we are in the wellness and health business, we are still in the sickness business," and that reality raises the stakes for every operational and technology decision a health system makes. As a result, buyers are not only asking, "How much upside does this create?" They are also asking, "What could go wrong, and how bad would it be if it did?"

Health systems do not buy the way startups do. They do not optimize for speed, novelty, or theoretical ROI alone. They optimize for continuity, reliability, and the absence of negative outcomes, which is exactly what AHRQ's work on workflow and safety highlights. Their buyers operate under a simple but powerful principle: do no harm. That mindset shapes procurement timelines, pilot requirements, and why promising solutions sometimes stall before full adoption.

The Health System Buyer's Mental Model

Every significant health system decision sits at the intersection of four risks: clinical harm, operational disruption, financial exposure, and reputational damage.

Even small documentation or order entry changes can increase missed steps and errors linked to preventable adverse events. On the operational and financial side, downtime analyses estimate that hospitals experience multiple significant outages per year, totaling 10 to 24 hours of disruption. The financial impact can average around 7,500 dollars per minute, and as much as 25,000 dollars per minute for large systems. Medium sized hospitals can lose approximately 1.7 million dollars per hour of outage. Large hospitals can lose as much as 3.2 million dollars per hour.

Reputational risk is tightly bound to cybersecurity. Recent reports indicate that 92 percent of surveyed healthcare organizations experienced at least one cyberattack in the past year, with an average of 40 attacks per organization. A 2025 summary from the HIPAA Journal, based on IBM's Cost of a Data Breach Report, estimates the average U.S. healthcare breach at 7.42 million dollars, the highest of any industry for more than a decade. Outages and breaches are not just financial events. Studies link them to delayed care, medical errors, and in some cases worse clinical outcomes.

In this environment, upside that is not paired with a credible safety story often gets discounted. A solution that promises efficiency but introduces even a small probability of downtime, workflow confusion, or breach risk will face significant resistance. A solution that clearly reduces those risks tends to gain internal momentum more quickly. ROI is important. But risk needs to be clearly understood and managed first.

IT Platforms: The Fear of Taking Systems Offline

This mindset becomes clearest in healthcare IT. Analyses of data performance and availability describe how slow or unreliable platforms cascade into delayed diagnostics, missing results, and clinician frustration. The same downtime studies quantify the impact: medium sized hospitals can lose about 1.7 million dollars per hour of outage, and large hospitals as much as 3.2 million dollars per hour when core systems are down.

Installing or upgrading a platform is not just a technical exercise. It is a change that directly affects uptime, data integrity, and clinician trust. Nursing and risk management groups point out that downtime and manual workarounds increase the risk of medication errors, missed or duplicated orders, and communication breakdowns. Health systems know that temporary disruption can become lasting friction. A system that technically works but slows clinicians or forces awkward workarounds can create new risks, which is exactly what AHRQ's workflow guidance warns about.

That is why buyers care deeply about how long systems will be offline or degraded. They scrutinize testing protocols, pilot environments, cutover

plans, and rollback strategies. They want to know what happens at two in the morning when something fails. Analyses of real incidents stress that organizations with clear cutover plans, rollback strategies, and rehearsed incident response recover faster and with less clinical impact. Promising speed without demonstrating safety is a red flag. Sellers who gloss over implementation risk may generate early excitement, but rarely achieve sustained adoption.

Clinical Technology and Protocols: Proof Before Scale

The same dynamic applies to clinical technology and new care protocols. In the Journal of the American Medical Informatics Association, Blumenthal and colleagues show that better clinical data sharing improves patient safety indicators and helps identify high risk medication use, while fragmented data undermines quality measurement and decision making. Their work underscores that new clinical tools must be evaluated for how they affect data completeness and reliability at the point of care, not just how impressive they look in a demo.

AHRQ's "Measuring Clinical Workflow to Improve Quality and Safety" emphasizes that organizations need to measure how new systems change real workflows and monitor for unintended consequences over time. Pilots, trials, and phased rollouts are how health systems validate performance across patient populations, surface hidden risks, and build clinician confidence before committing to scale. From the health system's perspective, validation, training, workflow mapping, and monitoring are part of the product. They are how harm is prevented and trust is earned.

Cybersecurity: Always Present, Always Under Attack

Cybersecurity has moved from a background concern to a central feature in almost every healthcare buying decision. Recent statistics show that 92 percent of organizations experienced at least one cyberattack, that ransomware attacks nearly doubled compared with 2021, and that more than half of organizations dealing with data loss reported disruptions to patient care and, in some cases, higher mortality. Breach cost reports show that healthcare has led all industries in average breach cost for 14 consecutive years, with U.S. incidents averaging around 7.42 million dollars in 2025.

Security focused firms describe downtime as a 7,500 dollar per minute crisis, driven by a combination of cyberattacks, IT failures, and vendor issues. Their analyses highlight that poorly governed third party access is a recurring factor in major incidents and that each new vendor connection represents another potential weak link. For health system buyers, that translates into a practical rule: any solution that introduces ambiguous access pathways, unclear incident response responsibilities, or weak controls will face intense

scrutiny, no matter how strong its ROI story looks. On Healthcare Rap, physician and AI leader Justin Norden captured the stakes succinctly: “Trust is everything in healthcare,” and that applies as much to digital tools and data flows as it does to in person care.

How to Best Lean Into These Interests to Demonstrate Value
For healthcare B2B sellers, the implication is straightforward: lead with safety, then build the case for upside. The AHRQ workflow work and the JAMIA research both suggest that technology that preserves or improves safety and fits existing workflows is far more likely to see sustained adoption than tools that simply promise efficiency gains. Effective sellers mirror that thinking and frame their value through the same risk lens their buyers use.

Effective sellers consistently reinforce three things:

1. **This will not cause harm.** They show how patient safety, clinical workflows, and data integrity are protected. They provide specific safeguards, controls, and examples from comparable environments.
2. **This will be implemented with minimal disruption.** They walk through pilots, testing phases, implementation timelines, cutover plans, and rollback strategies. They demonstrate experience in environments just as complex.
3. **When things go wrong, we will be there, fast and with the right people.** They outline support models, escalation paths, and real human accountability. Buyers care deeply about response capability, especially in high risk environments.

Health system digital leaders say the same thing in their own words. Franco Cardillo, executive director of digital strategy and operations at MUSC, told Healthcare Rap that his personal brand “is either going to hurt or help the installation of something,” and that success depends on showing teams “you are going to walk alongside them” through change rather than dropping technology on them from above.

Censinet’s downtime analysis, the HIPAA Journal’s cost data, and cybersecurity statistics all give sellers credible numbers they can use to anchor these conversations and quantify what failure looks like. When vendors lead with that reality, safety stops being a constraint and becomes a differentiator.

The Real Decider
Health systems adopt what they trust. They trust what feels safe. In healthcare B2B sales, the offers that win are not just the flashiest or the fastest to demo. They are the ones that make executives, clinicians, and

security leaders confident that patients, staff, and data will be safer and more stable than before.

In that context, safety is not boring. It is attractive. It is reassuring. And for buyers who manage risk every day, it is genuinely compelling.

Acknowledgements & Citations
This report draws insights and direct quotes from:

- Blumenthal, D., et al. “Clinical data sharing improves quality measurement and patient safety.” Journal of the American Medical Informatics Association, 2021.
- Censinet. “Healthcare Downtime Costs Hospitals 7,500 Per Minute on Average.” 2025.
- Censinet. “The Hidden Costs of HIPAA Violations: Clinical Downtime and Lost Trust.” 2025.
- Gosling, A. S., et al. “Patient Care Technology Disruptions Associated With the Implementation of Clinical Information Systems.” 2025.
- HIPAA Journal. “Average Cost of a Healthcare Data Breach Falls to 7.42 Million.” 2025.
- HIPAA Journal. “Healthcare Data Breach Statistics.” 2026 update.
- IS Partners, LLC. “Healthcare Cybersecurity Statistics 2024.” 2025 update.
- National Library of Medicine / AHRQ. “Measuring Clinical Workflow to Improve Quality and Safety.” 2020.
- Silk. “When Healthcare Data Performance Impacts Patient Safety.” 2026.
- Symmetric IT Group. “Healthcare IT Downtime: Enhancing Patient Safety and Efficiency.” 2025.
- Texas Nurses Association. “Impact of Hospital Downtime on Patient Safety: Are You Engaging Your Risk Management Department?” 2025.
- Houston Tech. “The Cost of Downtime in Healthcare: Why IT Resilience Is No Longer Optional.” 2025.
- Healthcare Rap, Episode 401: Joey Seliski of Allegheny Health Network and Franco Cardillo of MUSC, March 14, 2025.
- Healthcare Rap, Episode 414: Peter Chang of Tampa General Hospital, April 19, 2025.
- Healthcare Rap, Episode 440: Justin Norden of Qualified Health, August 12, 2025.