The Tipping Point

The State of Technology in Value-Based Care

2025 Report

Despite unprecedented agreement among healthcare leaders on the importance of artificial intelligence and technology, persistent gaps remain in deploying these tools. We stand at a crossroads where implementation will determine the future of value-based care.

reveleer

Mathematica
Progress Together

Contents

Figures

Executive summary

As healthcare continues to shift from fee-for-service to value-based care (VBC), payers and providers are rethinking their playbooks to deliver better quality, enhance patient results, and slash costs. Technology drives this change, helping organizations wrangle complex data, streamline care coordination, and connect legacy systems, all to enhance patient care.

To dig deeper into technology's impact on VBC, Reveleer, The Harris Poll and Mathematica surveyed over 200 directors, executives, and C-suite leaders about how they handle data, harness artificial intelligence (AI), and manage cybersecurity. We also asked what gives them a competitive edge—and what roadblocks still stand in their way.

The results revealed what many in our industry already know. Industry leaders agree on VBC objectives, persistent challenges in implementation remain.

Key findings

Provider and payer organizations naturally have different objectives based on their roles. But both acknowledge the relevance of data management, the impact of AI on return on investment, and the need for strong cybersecurity infrastructure.

Figure 1. Providers and payers agree that technology in VBC matters.

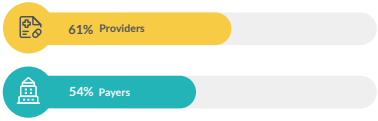
Both providers (97%) and payers (96%) agree that having a strong data management approach provides their organization with a competitive edge in the marketplace.

Ninety-six percent of providers and payers agree that their organization's approach to AI adoption and implementation has provided a competitive advantage over others in the market.

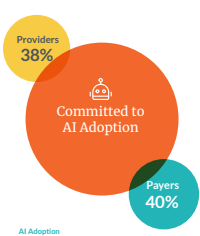
Fifty percent of providers and 49% of payers identify data security as the top priority for improving data management capabilities over the next twelve months.

Across the board, providers and payers recognize the importance of technology in VBC and have adopted AI to some degree. However, some are taking the lead by making a deeper commitment to fully drawing on AI to meet their goals.

Figure 2. Despite its importance, adoption of technology in VBC lags.



61% of providers and 54% of payers describe technology as very important to the success of their organization's VBC initiatives and practice.



AI Adoption
***38% of providers and 40% of payers** are committed to AI adoption.*

Cybersecurity threats
***56% of providers and 47% of payers** feel very prepared to handle cybersecurity threats.*

Methodology

The Harris Poll conducted this research online in the United States, surveying 203 U.S. residents and full-time employed workers. Respondents were ages 21 and older, had a job title of director or above; worked for a U.S.-based organization that used a VBC model; and were decision makers in audits and compliance, clinical informatics, clinical documentation improvement, member or patient enrollment, medical record retrieval, risk adjustment, or information technology and security. The survey took place from May 27 to June 10, 2025.

Respondents are divided between:

We defined providers as (1) organizations delivering care directly to patients or (2) respondents who work in a healthcare organization with 25 employees or more. Providers must also have worked in a hospital, physician group, integrated health system, accountable care organization (ACO) or ACO enabler, dialysis organization, integrated provider network, home and community-based care organization, healthcare enabler organization, or home healthcare agency. We defined payers as (1) organizations that cover medical services or (2) respondents who work in the insurance industry and in a commercial health insurance company, government health program, or managed care organization. Raw data were not weighted and therefore represent only the people who completed the survey.

We selected survey respondents from among people who have agreed to participate in Harris Poll surveys. The sampling precision of Harris online polls is measured using a Bayesian credible interval. For this study, the sample data are accurate to within ± 6.8 percentage points using a 95% confidence level. This credible interval will be wider among subsets of the surveyed population of interest.

All sample surveys and polls, whether or not they use probability sampling, are subject to other errors that are often not possible to quantify or estimate, including errors related to coverage, nonresponse, question wording and response options, and post-survey weighting and adjustments.

Introduction

Value-based care (VBC) is reshaping how we deliver and pay for healthcare in the US. As of January 1, 2025, the Medicare Shared Savings Program (MSSP), the largest accountable care program in the country, served 11.2 million beneficiaries alone (Centers for Medicare & Medicaid Services [CMS] 2025a).

A growing number of providers and payers are committing to the goal of achieving better outcomes at a lower cost through VBC, including through federal healthcare models and programs such as Medicare Advantage, state Medicaid programs and managed care, and commercial programs. Achieving that goal, however, depends on a strong technological foundation to build a complete picture of quality at the patient and population level, with accurate data and effective information sharing.

Building that foundation is far from simple. Healthcare organizations must navigate a complex landscape of fragmented systems, evolving technology such as artificial intelligence (AI), and increasingly sophisticated cybersecurity threats. Improving outcomes under VBC models also requires the ability to measure the patient and population health journey before, during, and after interventions, using systems that effectively collect, convey, and use this information.

Part of the challenge is that providers and payers see different parts of the data picture. Payers often have access to a broad set of population data, while providers track detailed, patient-level data. But when supported by modern data infrastructure and the right technology, these two perspectives combined can shed light on what's working today and uncover new innovations, ready to scale.

Federal policy is also pushing the industry forward. The Centers for Medicare & Medicaid Services (CMS) and technology companies are committing to collaborating on updated policy standards for digital health management, interoperability, and health information exchange **(CMS 2025b)**. With technology-forward policies gaining momentum, healthcare leaders face growing pressure to ensure safe, secure, and standards-aligned data management and sharing practices.

Some organizations are moving quickly. Using technology to generate clinical insights, automate manual processes, and strengthen data protection to safeguard patient privacy, they are advancing their VBC models and setting the pace for others. Still, many are in the early stages of adoption and working to build the internal capacity and confidence needed to turn strategy into measurable impact.

To get a clearer picture of how healthcare organizations are managing the complexities of VBC amid rapid digital change, we surveyed 203 leaders from provider and payer organizations. Their responses offer real-world insights into how technology is driving progress, and where things are still getting stuck.

Figure 3. Understanding the growth of VBC.

Note: We used MSSP shared savings as a proxy for the growth of Value-Based Care. These numbers do not include the beneficiaries served by other Medicare initiatives, including Medicare Advantage; Medicaid; or commercial insurers.

Source: CMS. "Program Data." Modified January 15, 2025.

As VBC cements its place at the forefront of healthcare delivery, organizations must navigate a landscape defined by change, innovation, and increased accountability. The next sections of this report delve into how healthcare leaders are responding to these shifts—describing current strategies, anticipated challenges, and useful insights that can empower organizations to thrive in a value-driven era.

Data Management

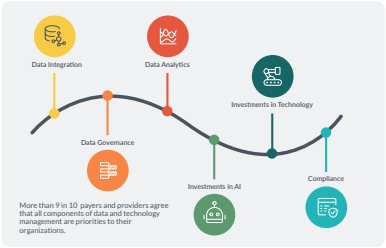
Healthcare leaders seek a mature approach to data management

Data Management

Healthcare leaders agree: they need a strong, well-rounded data management approach to deliver on obligations to consumers and shareholders. Survey responses suggest they see all elements of data management as equally important and complementary, with each component enhancing the effectiveness of the others. Comprehensive data integration, for example, enables more insightful data analytics. And high-quality, well-managed data lay the groundwork for advanced technology such as AI and safeguards such as cybersecurity.

Figure 4. Providers and payers likely to invest in data management for a competitive edge.

Figure 5. More than 9 in 10 payers and providers agree that all components of data and technology management are priorities to their organizations.



The priorities for achieving value-based care business goals include: data integration, data governance, data analytics, investments in AI, investments in technology, and compliance.

Data management foundations are in place, but operational gaps remain. Most VBC leaders agree that having a strong data management approach gives them a competitive edge and have plans to invest in data management technologies in the next 12 months. And while they're confident in the completeness and accuracy of their data, they still face challenges using that data in system-level operations.

- Only about one-third of leaders: (33% of providers and 31% of payers) rate their ability to **integrate data across systems** as excellent.
- Seven in 10 leaders: (73% of providers and 75% of payers) say technology platforms are **too complex or time-consuming for providers to use technology effectively.**
- Eight in 10 leaders: (85% of providers and 86% of payers) say there are **too many manual processes in their organization's VBC workflows.**

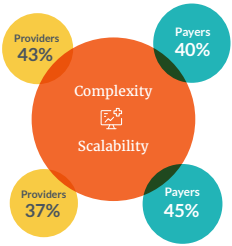
These challenges in using data in system-level operations reveal areas where VBC organizations must use to close the gap between data management expectations and typical data management inefficiencies.

Figure 6a. The roadblocks to interoperability—data quality, security, and complexity.

Data Quality
***40% of providers and 50% of payers** rank data quality issues as a top challenge to integrate data across systems.*

Data Security
***55% of providers and 56% of payers** rank data security concerns as a top challenge to integrate data across systems.*

Figure 6b. Complex data formats inhibit effective scaling.



Complexity
***43% of providers and 40% of payers** rank complexity issues as a top challenge for standardizing data formats across systems.*

Scalability
***37% of providers and 45% of payers** rank scalability issues as a top challenge for standardizing data formats across systems.*

Despite leaders' focus on data management, two key challenges persist: (1) many organizations struggle to use data smoothly for both clinical and business tasks, and (2) ongoing issues with data quality hinder effective integration. To bridge the gap between expectations and reality, organizations might need to further improve data systems and quality—potentially with support from policy initiatives designed to establish universal standards across the healthcare industry.

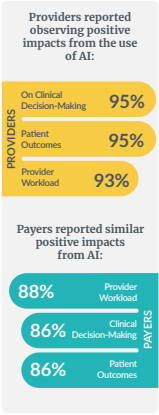
Artificial Intelligence

Although VBC leaders recognize AI's value, widespread commitment remains elusive

Artificial Intelligence

Across the VBC industry, organizations are finding a home for AI in their daily operations. Leaders from both payer and provider organizations believe AI and advanced analytics will be key to succeeding in VBC and that their organization's approach to AI adoption and implementation gives them an advantage over their competitors. Leaders also agree on the strong business case for AI and that their organization's AI use has a growing return on investment.

Figure 7. Positive impacts of AI.



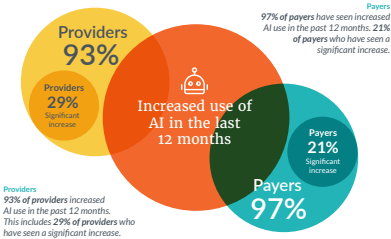
Despite recognizing AI's potential, some healthcare organizations are reluctant to commit. Only 38% of providers and 40% of payers say their organizations are fully committed to AI adoption, and even fewer—only 29% of providers and 21% of payers—have seen significant increases in AI use compared to 12 months ago. Hesitation is understandable, as AI adoption introduces new security, operational, and investment-related risks. To address this hesitation, many investors are now prioritizing solutions backed by evidence of sustainable impact in real-word healthcare settings, and healthcare researchers are working to develop frameworks to help organizations assess their return on investments **(PitchBook 2025)**.

Although full-scale adoption might take time, healthcare organizations that act on AI today have a chance to define what effective, responsible use looks like for VBC in the years ahead.

> *AI adoption in healthcare comes with high stakes. When people's health and well-being are on the line, innovation must be balanced with appropriate caution."*

Ngan MacDonald,
Director Data Innovation Lab at Mathematica
Better Data Will Pave the Path for AI-Powered Healthcare

Figure 8. The AI business case: As AI picks up steam, the market is reporting positive outcomes.



Three beliefs driving AI adoption:

1

Advanced Analytics
Providers and payers (98% of both) believe AI and advanced analytics will be essential to succeeding in VBC.

AI Adoption
More than 9 out of 10 providers and payers agree that their organization's approach to AI adoption and implementation gives them an advantage over their competitors.

2

3

Return on Investment
Most providers and payers agree (97% providers, 96% payers) that their organization's use of AI has a growing return on investment in VBC models, with 43% of payers and 45% of providers strongly agreeing.

Setting new standards in VBC with effective AI strategies.

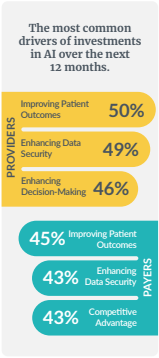
VBC payers and providers use AI in similar ways, suggesting both groups have a desire to improve point-of-care delivery, clinical decision making, and strategic planning.

1. Point-of-care

Healthcare leaders underscore the importance of optimizing clinical care processes to increase efficiency and foster more meaningful patient interactions. Providers (97%) and payers (96%) agree that using AI to help with point-of-care insights contributes to better patient outcomes in value-based care populations. For example, while nearly all payers (99%) and providers (100%) are likely to invest in AI technology in the next 12 months, providers appear particularly enthusiastic: 54% of providers are very likely to invest in AI over the next 12 months, compared to 46% of payers. There is also overlap between payers and providers in AI investments, with improving patient outcomes and enhancing data security being the most common drivers for both.

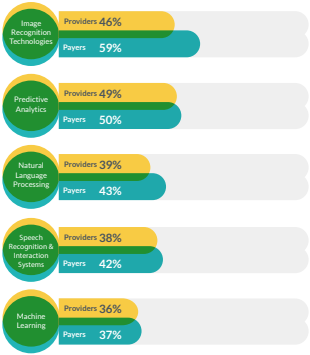
Leading organizations are harnessing AI's transformative power to deliver smarter, more connected care experiences. Both payers and providers are integrating innovative solutions such as AI-driven telemedicine, advanced predictive analytics, and next-generation diagnostic tools to elevate the quality of care and streamline workflow.

Figure 9. Agreement on the most common drivers of AI investment over the next 12 months.



Decision-makers highlight the tangible impact of these technologies—expanding access to services, accelerating early detection, and empowering clinical teams to intervene sooner for improved patient outcomes. By embracing these advancements, healthcare leaders are charting a course toward greater efficiency, precision, and value for the populations they serve.

Figure 10. Most popular AI tools among payers and providers.



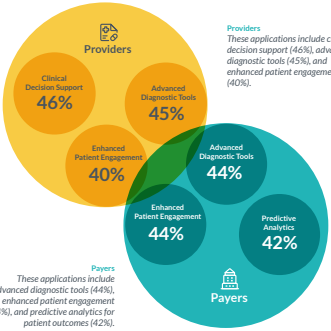
> ***"Predictive analytics enables proactive care, reducing hospital readmissions and improving chronic disease management by anticipating and addressing patient health risks early."***
>
> Survey Respondent
> *Vice President at a Provider Organization*

2. Advanced diagnostics

Providers and payers differ somewhat on the emerging AI applications they expect will affect VBC over the next two or three years. But both groups see an opportunity in advanced diagnostic tools and technology for enhanced patient engagement.

To improve patient engagement, leaders also cited specific use cases to illustrate the impact AI technology can have. For example, several respondents saw improved diabetes management outcomes after introducing wearable glucose monitors, which often use AI to process patient data and predict outcomes. Another organization noted that tools enabling patient engagement increase patients' participation in their own care. Patient portals are now commonly using AI with features such as virtual health assistants and chat bots.

Figure 11. Advanced diagnostic tools and technology for enhanced patient engagement rank among the top AI tools for providers and payers.



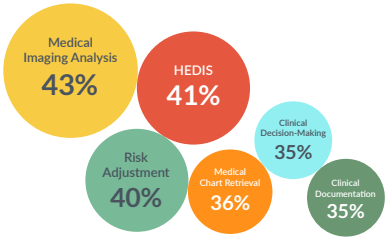
Providers
These applications include clinical decision support (46%), advanced diagnostic tools (45%), and enhanced patient engagement (40%).

Payers
These applications include advanced diagnostic tools (44%), enhanced patient engagement (44%), and predictive analytics for patient outcomes (42%).

3. Automating recurring activities

Payers and providers also see the potential impact of automating recurring analytical and management processes. Medical imaging analysis and risk adjustment are the two most common AI applications for both providers and payers, highlighting AI's role in diagnostic support at the patient and population levels. Payers and providers also use AI to support management and financial operations, reporting positive impacts from AI on operational efficiency, predictive modeling, and the overall costs of administering VBC models.

Figure 12. Total usage of most common AI tools for operational efficiency among payers and providers.



Providers
Medical imaging analysis: 48%
Healthcare Effectiveness Data and Information Set (HEDIS): 34%
Risk Adjustment: 43%
Medical chart retrieval: 36%
Clinical decision-making 40%
General clinical documentation 36%

Payers
Medical imaging analysis: 39%
Healthcare Effectiveness Data and Information Set (HEDIS): 49%
Risk Adjustment: 37%
Medical chart retrieval: 37%
Clinical decision-making: 31%
General clinical documentation: 35%

These results are encouraging and demonstrate that AI has already begun to reshape core aspects of value-based care, delivering tangible benefits for both payers and providers. However, as organizations move from early wins to deeper integration, the journey is rarely straightforward. The next phase is defined not by optimism alone, but by the capacity to navigate persistent obstacles that can hinder the full realization of AI's promise.

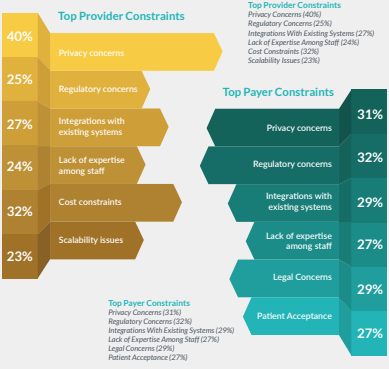
Figure 13. Healthcare leaders are beginning to recognize the positive impacts of AI.

> *"Machine learning algorithms detected risk patterns, enabling proactive care strategies."*
>
> Anonymous respondent
> *VP Provider*

Navigating the roadblocks of AI adoption

Although enthusiasm for AI's transformative potential is high, organizations quickly discover that realizing these benefits is not a straightforward process. The rapid adoption of AI among payers and providers highlights a critical challenge: the need to successfully integrate AI with legacy systems and to foster cultural change within organizations to promote responsible and ethical implementation.

Figure 14. Payers and provider agreement on the most common constraints to adopting AI technology.

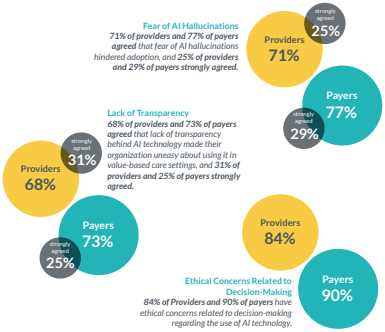


Innovating through uncertainty

A cultural shift is rapidly unfolding as AI becomes more integrated into the business landscape. In healthcare, enthusiasm for AI's potential to improve efficiency is tempered by concerns about its risks. Historically, healthcare technology has relied on deterministic, rule-based systems. The emerging acceptance of generative AI—probabilistic and powerful—requires careful consideration of the trade-offs between improved healthcare delivery and possible unintended harms.

Payer and provider concerns around AI adoption reflect ongoing discourse in the broader healthcare and technology industries related to fear of AI hallucinations, transparency in algorithms, and possible ethical concerns. Given the success payers and providers have found in leveraging AI across their VBC portfolio, this suggests a strong change management strategy is required to adopt AI successfully.

Figure 15. AI adoption in healthcare: challenges, concerns, and organizational responses.



Do your homework.

Only around 3 in 10 organizations provide extensive AI training (32% of providers and 30% of payers).

All provider and payer organizations are training their employees in the use of AI.

Leaning in to educating your workforce on appropriate AI use is important to overcoming common concerns and barriers for adoption.

As risk-bearing organizations embrace AI, it's clear that the path forward isn't without hurdles. Tackling issues like decisions made without enough human oversight, murky accountability, and lack of transparency isn't just important, it's crucial. Confronting these challenges head-on is the key to earning trust and unlocking the full potential of AI for succeeding in VBC.

Cybersecurity

Navigating the illusion of readiness

Cybersecurity

Despite general feelings of preparedness among VBC organizations, security breaches remain a present and costly risk. All payers and providers feel somewhat or very prepared to handle cybersecurity threats, although providers are more likely to feel very prepared (56% of providers, 47% of payers). Most payers (67%) and providers (68%) also report having tested their incident response plan in the past 12 months.

Figure 16. Rethinking cybersecurity preparedness.

52%

Feel "Very Prepared"
Despite 100% of organizations feeling prepared, only half express high confidence in their defenses against sophisticated attacks.

67%

Tested Response Plan
Two-thirds of organizations have tested their incident response plans within the last year, indicating active risk management.

29%

Providers Breached
Roughly a quarter of providers (24%) and a third of payers (34%) suffer a significant cybersecurity incident, highlighting persistent vulnerabilities.

However, costly cyberattacks persist across the healthcare industry, reinforcing warnings from cybersecurity experts that healthcare leaders should ask when, not if, an attack is imminent. Through the first seven months of 2025 alone, the U.S. Department of Health and Human Services (HHS) received reports of 374 breaches of unsecured protected health information—several of which made headlines—affecting over 35 million people **(Office for Civil Rights 2025; Southwick 2025; Muoio 2025; Identify Theft Resource Center 2025)**. Survey responses reflect this: about one-quarter of providers (24%) and one-third of payers (34%) report major cybersecurity incidents in the past 12 months.

The costs of a single security breach can be substantial. The impact of a breach—measured by the number of patient records compromised—has surged since 2019, largely driven by several mega-breaches affecting millions of people per incident. Most breaches result from hacking or information technology (IT) incidents, with business associates (vendors) increasingly representing the vector for mass-impact events **(Alder 2025)**.

Although the prospect of a breach can be daunting, our survey responses suggest steps healthcare leaders can take to ensure data systems are strong and secure.

Figure 17. Cybersecurity readiness checklist for IT Leaders.

Work with your IT team to ensure your systems are prepared for the greatest emerging cybersecurity threats that pose a risk to value-based care model operations. Below is a list of security considerations based on our survey findings:

- ☐ **Prioritize defending against data breaches by strengthening access controls and system monitoring.**
  > *Data breaches were identified as a great risk among emerging cybersecurity threats, cited by 61% of payers and 55% of providers, underscoring the importance of robust detection and prevention measures.*
- ☐ **Implement rigorous anti-phishing education and tools across your organization.**
  > *Phishing was identified as one of the greatest threats by 54% of payers and 47% of providers, showing the need for ongoing awareness training and advanced filtering technologies.*
- ☐ **Adopt comprehensive data leak prevention strategies, including encryption and audit trails.**
  > *Both payers and providers (51% each) named data leaks as a leading concern, emphasizing the value of strong data protection policies.*
- ☐ **Address insider threats through enhanced employee monitoring and clear security protocols.**
  > *Insider threats were identified as one of the greatest risks for 51% of payers and 42% of providers, highlighting the necessity for internal safeguards and accountability.*
- ☐ **Develop and routinely update a ransomware response plan.**
  > *Ransomware remains a great threat, noted by 41% of payers and 44% of providers, making it essential to build resilience and establish recovery procedures before an attack occurs.*

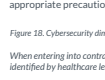
When assessing secure data integration strategies with electronic health records and third-party technology partners, organizations often look to leading industry practices. Data encryption stands out as the predominant approach, with 65% of payers and 74% of providers adopting it to safeguard sensitive information. In addition, endpoint protection remains a core layer of defense, implemented by 65% of payers and 55% of providers to further mitigate risk.

Interestingly, the third most prevalent method for securing data integration varies between sectors. Most providers (56%) conduct regular security assessments to identify vulnerabilities and ensure ongoing compliance with evolving standards. Payers, in addition to regular security assessments, also commonly utilize secure APIs (56%) to maintain rigorous control over the transmission and accessibility of patient data. Together, these strategies illustrate the multifaceted efforts organizations undertake to protect health information in a complex digital landscape.

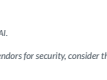
AI introduces a new set of cybersecurity challenges by increasing the "surface" of vulnerability at an organization. AI use may lead to security breaches similar to third-party partner breaches if organizations "trust" the technology without taking appropriate precautions.

Figure 18. Cybersecurity dimensions to AI.

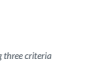
When entering into contracts with vendors for security, consider the following three criteria identified by healthcare leaders.



*Secure data storage, cited by **49% of payers and 50% of providers.***



*Regular security audits, cited by **36% of payers and 44% of providers.***



*Data breach notifications, cited by **37% of payers**, and data integrity measures, cited by **44% of providers.***

When evaluating potential vendors for healthcare technology solutions, one of the most valuable indicators of robust security practices is the presence of Health Information Trust Alliance (HITRUST) certification. Recognized as a gold standard across the industry, HITRUST certification demonstrates that a vendor has undergone comprehensive, rigorous assessment of its information security management systems and practices. By prioritizing vendors with HITRUST credentials, healthcare organizations can better ensure that proper security protocols are embedded into every aspect of data management, privacy, and risk mitigation. This not only helps organizations meet regulatory requirements, but also builds a foundation of trust with patients and partners, protecting sensitive health information amid evolving cybersecurity threats. After establishing HITRUST, organizations should implement continuous monitoring procedures to ensure safeguards are operating as intended.

Conclusion

VBC is no longer a future aspiration but the present reality. However, our survey elicits a central contradiction: although providers and payers are more aligned than ever before, collaboration and execution on technology adoption remain inconsistent. The goals are mutual, the tech is available, and yet the value-based care industry risks stalling just as momentum peaks. Without action, growth in VBC contracts and confidence in data and technology won't translate into meaningful, scalable improvements in care quality or outcomes.

Industry leaders widely acknowledge that data provide a competitive advantage, but siloed systems and quality challenges continue to block its full utility. Payers and providers broadly adopt AI, but trust gaps, limited training, and governance shortfalls restrain its transformative power. Meanwhile, cybersecurity threats loom, underscoring the risks of payers and providers assuming readiness.

This is the industry's tipping point. To meet the ambitious goals of value-based care models to improve quality and decrease costs, healthcare executives must embrace promising, evidence-backed strategies and face challenges head-on to develop a complete and accurate picture of patient and population-health, safe-guarded from security and privacy threats. This includes investing in data management to advance systems from "good" to "great," applying data-backed AI solutions to problems, and pressure-testing security systems. Beyond strong decision-making to set the tone for technology's role within an organization's value-based care strategy, leaders must empower staff to leverage core technology to support their daily work, and to champion

To drive real progress in value-based care, leaders must act boldly. Use these targeted action steps to advance technology adoption and deliver meaningful improvements throughout your organization:

- **Prioritize data security and integrity:** Ensure secure data storage and robust integrity measures are foundational for all technology partnerships. Regularly conduct security audits and establish rapid breach-notification protocols to protect sensitive information and build trust with patients and partners.

- **Invest in advanced data management systems:** Switch from siloed, "good-enough" systems to integrated, high-quality data platforms. Advanced data systems are not only essential for a comprehensive and accurate understanding of patient and population health, but they also lay the groundwork for successful AI implementation. Reliable, high-quality data enables AI tools to function accurately, efficiently, and ethically—maximizing their utility in supporting VBC strategies.

- **Apply AI thoughtfully:** Embrace AI as a tool to streamline workflows, enhance decision making, and support staff. Begin by piloting AI in lower-risk environments to build trust and understanding, always pairing automation with human oversight to ensure accuracy and ethical compliance.
- **Empower and train staff:** Move beyond basic introductions to technology by offering extensive, hands-on training tailored to both clinical and administrative roles. Encourage staff to harness technology to make daily tasks more efficient, while cultivating change champions who drive adoption and ensure compliance with data and security standards.
- **Strengthen cybersecurity readiness:** Be proactive by conducting regular audits, establishing clear contingency plans (such as paper backups), and addressing both common and high-impact threats. Instill an organizational culture of vigilance, resilience, and preparedness.
- **Foster purposeful collaboration:** Bridge the gap between payers and providers by aligning technology priorities and sharing best practices. Engage policymakers, vendors, and internal leaders in creating standards and policies that drive interoperability and shared progress.
- **Go deep before going wide:** Focus resources on evidence-based strategies and proven technology solutions. Pilot innovative tools in targeted areas, measure outcomes rigorously, and scale what works.

By acting on these recommendations, healthcare leaders can resolve the challenges described in this report. Effective use of technology is not just a competitive advantage—it is key to improving quality, containing costs, and achieving the promise of VBC.

This report captures where we are today so we can illuminate the path forward together. By advancing digital adoption, strengthening data integrity, and fostering collaboration across all stakeholders, healthcare leaders can redefine what's possible. With bold vision and unwavering commitment, the sector can turn today's momentum into lasting transformation, setting new standards for quality, efficiency, and equity in care. The next era of VBC is within reach, powered by innovation and inspired leadership.

About

As the industry's pioneering VBC enablement partner, Reveleer is built to solve the most pressing real-world challenges faced by provider and health-plan organizations today. By unifying retrieval, clinical intelligence, risk adjustment, quality improvement, and member management solutions into one intelligent, AI-powered system, Reveleer streamlines fragmented workflows to supercharge productivity, enhance care quality, and optimize performance on high-priority value-based initiatives. To learn more, visit https://www.reveleer.com/.

Mathematica works with public, private, and philanthropic organizations to make programs and policies more effective, efficient, and impactful—with action-ready evidence, scalable data solutions, and insights that drive results. The Mathematica team includes data scientists, social scientists, technologists, and policy experts that bring an integrated approach to solving tough public and private sector challenges. To learn more, visit https://mathematica.org/.

The Harris Poll is a global public opinion, analytics, and market research consultancy that strives to reveal society's authentic values to inspire leaders to create a better tomorrow. With a global research reach of more than 90 countries, Harris offers advisory services across sectors to world leaders, CEOs, and business decision-makers with state-of-the-art analytics, real-time software services, and practitioners in marketing, reputation, customer experience, trends, futures, and thought leadership/research-for-public release, The Harris Poll translates shifting social sentiment into a competitive marketplace advantage. The Harris Poll has tracked public opinion, motivations and social sentiment since 1963. Harris is a Stagwell (NASDAQ: STGW) company. www.theharrispoll.com.

References

CMS. "CMS Moves Closer to Accountable Care Goals with 2025 ACO Initiatives." 2025b. https://www.cms.gov/newsroom/fact-sheets/cms-moves-closer-accountable-care-goals-2025-aco-initiatives.

CMS. "Shared Savings Program Fast Facts—As of January 1st, 2025." 2025a. https://www.cms.gov/files/document/2025-shared-savings-program-fast-facts.pdf.

Identify Theft Resource Center. "ITRC H1 2025 Data Breach Report." 2025. https://www.idtheftcenter.org/publication/itrc-h1-2025-data-breach-report/.

Muoio, D. "Oracle Health Server Breach Leads to Hospital Extortions, Reports Say." Fierce Healthcare, 2025. https://www.fiercehealthcare.com/health-tech/unannounced-oracle-health-server-breach-leads-hospital-extortions-reports-say.

Office for Civil Rights, U.S. Department of Health and Human Services. "Breach Portal: Notice to the Secretary of HHS—Breach of Unsecured Protected Health Information." n.d. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

PitchBook. "AI Healthcare & Life Sciences VC Market Snapshot." 2025. https://files.pitchbook.com/website/files/pdf/2025_AI_Healthcare_Life_Sciences_VC_Market_Snapshot.pdf.

Southwick, R. "These Are the Biggest Health Data Breaches in the First Half of 2025." Chief Healthcare Executive, July 2025. https://www.chiefhealthcareexecutive.com/view/these-are-the-biggest-health-data-breaches-in-the-first-half-of-2025.

Alder, S. "Healthcare Data Breach Statistics" The HIPAA Journal, 2025. https://www.hipaajournal.com/healthcare-data-breach-statistics/.

State of Technology in Value Based Care 2025 Report

Reveleer.com