AMA
AMERICAN MEDICAL ASSOCIATION

# Investment in technology for value-based care

Guidance for physician practices

# Table of contents

# Introduction

Technology investments are a core strategic consideration for practices engaging in value-based care arrangements. These arrangements require a fundamentally distinct approach from the fee-for-service model to manage, track, and report the care provided to patients. Therefore, they often utilize different kinds of technology to promote success. For example, value-based care (VBC) arrangements often prompt practices to modify the ways they collect, analyze, document, and report the care provided to patients. They may also include new or enhanced incentives intended to change how a practice manages an identified patient population; practices with an incentive to manage a patient's overall health status may have greater motivation to invest in technologies to help them better track, monitor, promote, and improve that patient's health.

This document is intended to provide physicians and their practices with an introduction to some key concepts in vetting technologies that may assist in value-based care efforts and negotiating vendor agreements reflecting the same.

Some common examples of technology investments are below. Note that many tools or solutions address (or claim to address) multiple categories.

- *Electronic health record* (EHR) solutions to document patient care and help meet regulatory requirements
- *Analytic tools* to help physicians and their care teams understand their performance and identify opportunities or challenges
- *Documentation tools* to help physicians and their care teams efficiently and accurately collect and record relevant clinical and payment data in a compliant manner
- *Technological tools* to help physicians and their care teams improve the quality of care
- *Patient engagement* and *health improvement tools* to help patients monitor and manage their own health

Although technology is often a vital part of any value-based care arrangement, investments in technology carry risks as well. Some risk considerations include:

- Large capital investments, particularly as it relates to start-up costs
- Cultural and strategic fit, including the risk of burnout with new technologies and disruption of clinical workflows
- Ability to integrate seamlessly with existing or remaining technology infrastructure
- Alignment with longer term strategic goals, including relationships with key partners
- Data security
- Regulatory risks, including compliance with the Health Insurance Portability and Accountability Act ("**HIPAA**") and other privacy laws

Adding to the challenge, practices face a diverse, competitive marketplace for technology solutions and risk mitigation. How can a practice best evaluate tools given the thousands of options currently available and the rapid pace of new technologies and offerings coming to market every day?

As a crucial first step, practices should first evaluate the specific gap or need that is to be addressed. For example, is the practice attempting to implement or improve its documentation, augment data analytic capabilities, implement a new health intervention, report data, or integrate into systems used by clinical partners? Does the practice prefer a wholesale overhaul of its technology suite, or the addition or improvement of certain business functions?

This analysis may also require an assessment of the practice's overall value-based care goals. For example, if a practice is highly experienced with a specific VBC arrangement, it may have developed a robust set of technology-based solutions that are difficult to change or modify. Does it have latitude to implement a new "in-house" solution, or will it need to take other entities into account in implementing a solution? Does the practice intend to change its value-based strategy in the near future (for example, by moving to downside risk or targeting a new patient population)?

**Key consideration**

If the practice is working with a third party to collaborate on a value-based arrangement (like a VBC enablement "aggregator" entity), that partner will frequently dictate or heavily influence the tools that should be used.

# Common Types of VBC-Related Technologies Available to Practices

As indicated above, practices should start by evaluating their overall technological needs. Common considerations for value-based arrangements include the following:

## Electronic Health Records

**EMR or EHR?**

An EMR is, generally, a digital version of what would have previously been a patient's paper chart—medical history collected, maintained, and stored by or at a single practice or system's offices. It is a local system, designed to work most effectively for a single practice or clearly defined health care system. An EHR is much broader in scope in two ways: (1) it includes additional access or interface capabilities across various providers and health information systems; and (2) due to that capability, houses a much more comprehensive digital record of a patient's health journey.

Though electronic medical records ("**EMR(s)**") have been around for over 50 years,[1] the Health Information Technology for Economic and Clinical Health ("**HITECH**") Act of 2009 propelled them forward by creating incentives for practices adopting certified electronic health records (and later reductions in Medicare payments for failure to meaningfully use them).[2] EHRs are now nearly ubiquitous in medical practices, with nearly 90% of office-based physicians adopting some form of EMR and nearly 80% adopting full Certified Electronic Health Record Technology ("**CEHRT**").[3]

### Key consideration

The Medicare Quality Payment Program's "Promoting Interoperability" rules now require many practices to implement CEHRT or face penalties to Medicare Physician Fee Schedule payments.

An effective EHR is not merely a digital chart filing system—it can have enormous impacts on data structure and clinical workflow. Many EHR systems are also capable of supporting other care-related activities directly or indirectly through various interfaces, including evidence-based decision support, quality management, and outcomes reporting. EHR developers are increasingly exploring automation and augmented intelligence ("**AI**") use cases. EHRs may also support data reporting under VBC arrangements. For example, Medicare value-based care programs, including the Medicare Shared Savings Program ("**MSSP**"), have increasingly required or encouraged providers to report quality data using electronic clinical quality measures ("**eCQMs**") reported through CEHRT.

EHRs are increasingly developed to perform as one-stop shops. The transition to cloud-based systems have also made EHRs much more adaptable and scalable. Nevertheless, an EHR cannot (and should not) be all things. Other technologies must fulfill specific operational needs within an organization, which is why interoperability is a key factor in an effective EHR. An EHR may need to exchange information with other systems and organizations entirely. In an effort to promote interoperability, the 21st Century Cures Act required the US Department of Health and Human Services (HHS) to establish standards for certified interfacing technology (i.e., application programming interface, "**API**").[4]

EHRs are increasingly the backbone of practice efforts to participate in value-based care. Due to their flexibility and ease in collecting, aggregating, and transferring data, they are a vital source of information to value-based aggregator entities, partners, and payers. Many VBC strategies involve greater alignment and integration among the EHR systems of participants, in order to implement strategies like improved risk coding documentation using standardized processes. By the same token, a VBC strategy may require a practice to modify its EHR strategy by adopting a platform used by another partner (often a hospital participant) or by adding or changing modules or features used in the current EHR system. However, practices should evaluate the impact on practice finances, workflows, and employee satisfaction. Note that value-based care entities (or other participants in a VBC arrangement) can sometimes help providers transition between EHR vendors through financial or technical assistance.

### Case study

Hattiesburg Clinic is an independent physician group in Mississippi that leverages technology to achieve success in VBC. Hattiesburg Clinic worked directly with its EHR to analyze population health resources and utilization, cost data, and care team efficiency, leading to improved clinical outcomes, patient experience, and clinician satisfaction. Click here to learn more about Hattiesburg Clinic's use of technologies to enable VBC.

## Clinical Access Technologies and In-Home Care Options

Physicians are also exploring technological tools to support care delivery, including telehealth platforms, remote monitoring, and options to help patients manage their health. These technologies may be attractive to VBC arrangements for several reasons. First, by making access to care more convenient, these tools may increase the likelihood of patient adherence to a treatment plan (potentially improving clinical outcomes and reducing the likelihood of unplanned hospitalization or higher-acuity care) and increase patient satisfaction (often a key metric of success in VBC arrangements). As such, successful implementation of these tools may lead to direct improvement in the practice's ability to meet benchmark goals under VBC arrangements. Second, they may provide additional data or insights that can guide patient care by helping physicians monitor health status, identify opportunities to improve care delivery, and track performance under the VBC arrangement's cost and quality goals. Third, they can improve the efficiency and response times for health care interventions, allowing practices to be more proactive in addressing health care needs while maximizing limited resources.

Telehealth accelerated rapidly out of necessity during the COVID-19 pandemic to become a substantial part of many practices' strategy. Since that time, the availability and diversity of telehealth care delivery models has grown. Medicare defines "telehealth" to mean the use of telecommunications and information technology to provide access to health assessment, diagnosis, intervention, consultation, and supervision by permitting two-way, real-time interactive communication between the patient and the physician or practitioner at a distant site. However, vendors have implemented other kinds of services often called "telehealth," including asynchronous and audio-only tools.

### Key consideration

As of early 2025, Medicare covers many telehealth services (including most face-to-face services) outside of rural areas based on a temporary expansion of flexibilities adopted during the COVID-19 Public Health Emergency. However, Medicare also permanently covers other services under which a clinician furnishes care outside the physical presence of a patient, such as care coordination services and remote patient monitoring. Medicare Advantage plans, commercial payers, and some Accountable Care Organizations ("**ACOs**") may also continue to support telehealth services even after the Medicare fee-for-service flexibilities end. Telehealth coverage policy may be subject to significant change, including the kinds of services covered, the types of technology required, rules around prescribing, the allowable location of the patient and clinician, and parity of payment with in-office services.

Remote monitoring services provide an alternative way for physicians or other practitioners to collect data on patient health status. These technologies allow patients to submit data concerning elements of their health status ("remote patient monitoring" of health status indicators like blood pressure or oxygen saturation) or their progress in a therapeutic regimen ("remote *therapeutic* monitoring"). Similar to telehealth, rules for remote monitoring coverage may vary depending on the payer. However, note that Medicare will only pay for remote monitoring if the device used to collect and transmit relevant data meets the standard of a "medical device" under Food and Drug Administration ("**FDA**") rules.

### Billing and coding highlight

Certain "care management" services like chronic care management, principal care management, and transitional care management may incorporate patient outreach and communications tools, without technically being considered "telehealth" under applicable billing rules. Physicians should review the description of these services in the AMA's Current Procedural Terminology (CPT) and VBC Issue Brief.

### Key consideration

**Software as a medical device ("SaMD")** is "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device."[5] Such medical purposes can include interpreting information for diagnosis and treatment, continual collection of data through monitoring or active management, or proactive tools for prevention and wellness. Examples range from image analysis tools in a radiology office to glucometers worn continuously by a patient. SaMD is regulated by the FDA as a medical device, unless an exception applies. Therefore, it can be used to report data under the remote monitoring codes. However, because several exceptions and exclusions apply, it may be difficult to assess whether a technology – especially a new technology – fits the standard of a medical device, including SaMD.

Telehealth and remote monitoring investments raise a variety of legal and practical questions outside the scope of this summary. However, participants in value-based programs should understand the anticipated role of telehealth and similar services in any value-based arrangement. Implementation of these services may have important implications. For example, Medicare and some managed care plans will only accept risk coding of diagnoses conducted through a face-to-face visit. Although such visits can occur via live video telehealth (under current law), these rules are subject to frequent change, which could substantially alter a VBC provider's strategy to oversee, track, and document the health status of its patient population. As another example, certain value-based care arrangements like ACOs or MA arrangements can support telehealth services in ways that go beyond the Medicare fee-for-service program. ACOs may even go a step further and provide financial and in-kind support to purchase and implement the technological platform used. As still another example, ACOs and similar entities sometimes use telehealth to ensure they are providing adequate care to patients throughout their service area – including in rural and underserved regions.

Some key questions for practices evaluating telehealth and remote monitoring arrangements are the following:

- *What is your strategic goal in adopting telehealth and/or remote monitoring, or changing your vendor for these services, to support your VBC efforts?*

  Some practices use these technologies to expand existing offerings, improve patient experience, or increase geographic reach. Others develop full business models around telehealth or remote monitoring services, including virtual-only models. Practices should also consider whether these goals align with the goals of their value-based arrangement.

- *Are there any current constraints on your adoption of a telehealth or remote monitoring platform?*

  For example, if you are in a value-based arrangement with a hospital partner or an enablement entity, that partner may require use of their telehealth platform to increase integration. The VBC arrangement also may implement certain clinical or business workflows that assume (or require) consistent uses of the same technology platform.

- *What specific services will be provided through telehealth and remote monitoring?*

  Do you have assurances that they will be paid for even if payer policies change (for example, using ACO shared savings)?

- *Will an ACO or other partner support your implementation of the technology?*

  This may include many different kinds of support, including investments in hardware, support for software licenses (including SaMD tools), providing services related to implementing the technology into your workflow, and security tools.

- *If provided through a vendor or a value-based care enablement entity, what are the actual terms of service?*

  For example, some vendors provide services like chronic care management through personal service arrangements to support the practice's delivery of the service. Others provide turnkey solutions under which the vendor supplies all required personnel, supplies, and equipment under the overall direction of the practice.

For additional evaluation questions and other strategic insights, please see the AMA's Telehealth and RPM playbooks.

## Analytics and Practice Management Tools

As more data continues to become available to providers, more specialized techniques and tools emerge to access, analyze and extract insights from it. Often integrating with or extracting data from a practice's EHR (if not a function within the EHR itself), innovative tools can aggregate data from multiple disparate resources to track trends across different patient categories, analyze population health, and conduct risk stratification to better target care. Practice management tools, whether built into analytics platforms or used separately, track past and present performance metrics to identify strengths and opportunities for improvement in care and costs. They are also used to predict outcomes and model strategy adjustments for the future. In VBC arrangements, this data can also be used to establish benchmarks.

Analytic tools are essential to success under value-based care arrangements that incentivize improvement in costs, such as in Total Cost of Care (TCOC) arrangements. Robust data analysis allows participants in value-based arrangements to understand the relative costs, efficiency, and health effects of care delivered in different settings, characteristics of the patient population, and opportunities for health interventions. Certain entities like ACOs also receive special access to additional data reflecting the care provided to all patients by all providers (even those outside the ACO). These tools allow participants in value-based arrangements to assess costs on a per-patient basis over a certain time period (e.g., per-month or per-year), expenses per event or clinical episode, and measures of health status like a patient risk-adjustment score. This data can be further broken down into categories including disease profile, geography, and patterns of

accessing care (like tracking readmissions or preventable emergency department visits).[6] These insights then become the basis of improved management of the VBC arrangement's attributed patient population – the heart of any VBC strategy.

As with other technology solutions, practices will need to decide whether to develop an in-house or external data analytics capability. In-house data analysis may require the hiring of additional practice staff with specialized skills. Third-party analytics may be structured as an ongoing inquiry into practice data or a specific project reflected in a Statement of Work. Alternatively, the ACO or another value-based entity may have invested in its own data analytics capability as part of its overall infrastructure.

**Key consideration**

There are many sources of data that can be used for analysis. MSSP ACOs get quarterly data feeds reflecting their patients' overall Medicare experience. Other payers may also provide data concerning the care utilized by patients. Note that access to this data may require execution of other arrangements like the CMS Data Use Agreement. Although these additional arrangements are generally presented as form agreements that cannot be negotiated, practices should carefully review these documents because they often contain unique rules around the permitted uses and disclosures of the value-based care data, securing and destroying any data received, and the treatment of any materials created using this data.

## Augmented Intelligence-Based Tools

The health care technology industry has utilized various forms of machine learning and augmented intelligence ("**AI**") for years (and in some cases decades). The AMA has issued formal AMA policy on the use of AI going back to 2018.[7] With the sudden introduction and accessibility of "generative" capabilities in 2022-2023, a renewed focus and exploration of AI capabilities has emerged.

AI has enormous potential to transform health care payment and delivery, particularly in VBC arrangements. These arrangements often prompt physicians to collect information that goes beyond traditional medical recordkeeping, meet heightened documentation standards (often differing from fee-for-service standards), ingest and understand significant amounts of data, identify trends and opportunities in that data, predict cost implications, develop new intervention strategies, and evaluate those strategies. Participants in VBC arrangements have implemented AI-based tools to assist with many of these tasks. Such tools have particularly been used to speed up repetitive or time-consuming administrative tasks like drafting visit notes, maintaining health records, abstracting parts of the health record supporting medical necessity determinations, summarizing complex regulatory and coding rules, and assembling data to comply with quality reporting obligations. With its ability to aggregate and analyze staggering volumes of data quickly, AI can be used to help organizations identify patterns, opportunities, or challenges that may not be immediately evident. Some AI tools may also help physicians improve care coordination efforts and inform overall health management by efficiently (often automatically) combining data from numerous sources into digestible summaries of patients' wellness status. Improved documentation may also help physicians satisfy compliance obligations (for example, by documenting adherence to a treatment plan). Finally, AI-enabled "clinical decision support" tools may help validate or supplement physicians' decision-making capabilities, which may lead to improved outcomes. Predictive models may not only help identify potential health risks, but also behaviors, such as the likelihood a patient will schedule their annual check-up without additional outreach.

### Case study

Geisinger Health System is a large, regional healthcare system that utilizes AI to advance its VBC objectives through risk stratification, allocating system resources, and driving early, timely interventions. Click here to learn more about Geisinger Health's use of AI and other technologies to enable VBC.

### Limits of AI

AI is not, however, a magic wand. Grandiose representations about "AI" solutions became such a problem that, in 2024, the Federal Trade Commission stepped up enforcement against "operations that use AI hype" through false or misleading claims.[8]

### Limits of AI

Like any technology, AI may have implementation risks, especially if used outside expected parameters. Use of AI can potentially increase data privacy and security risks. Since it is only as good as the quality of the data it ingests, AI is susceptible to and can even amplify bias and other errors. AI models may be trained or tuned for a particular use case and perform poorly at others. Recognizing the potential and risks of AI, the AMA has issued several formal policies addressing the ethical use of AI in health care.[9]

In healthcare, the use of AI raises some important and complex legal and regulatory issues. While a full summary is outside the scope of this document, use of AI models raises questions about the security of protected health information, professional liability, general liability (including treatment of "hallucinations" or inaccurate information generated by AI models), and compliance with regulatory standards (including nondiscrimination rules). These issues can be even more complicated when a physician is part of a value-based arrangement involving several other entities. For example, who would be responsible for an adverse health outcome due to an error on the part of an ACO's AI-enabled vendor in analyzing a physician's documentation? AI has also become integrated into many payer processes, leading to fears of an AI "arms race" requiring ever more detailed documentation (also possibly generated via AI) to combat algorithmic claims denial processes.

AI is an intense focus of federal and state regulators, and rules surrounding the use of AI may change substantially over the lifecycle of an agreement. Physicians should ensure they understand the implications of any significant regulatory changes, particularly regarding their right to amend or modify a VBC agreement that incorporates an AI tool. For example, physicians may wish to include language in their agreement calling for the right to amendment upon any change to material legal or regulatory provisions, possibly even specifically calling out changes related to AI.

**Key consideration**

AI raises some particularly complicated issues under HIPAA and similar privacy laws. HIPAA prohibits the unauthorized use and disclosure of protected health information ("**PHI**"), as well as the sale of PHI, with some exceptions. PHI can only be used for certain functions like treatment, payment, operations, and research, and then only with the patient's authorization for the designated purpose. Practices' typical patient authorizations may not cover AI training, and it may be challenging to collect revised patient authorizations. HIPAA also requires practices to only collect the minimum necessary PHI for a particular purpose, which may be difficult to square with the need for voluminous data to train the AI model. Finally, access to PHI in exchange for payment may be deemed sale of PHI. Practices should carefully consider their HIPAA compliance strategy in working with AI-based products.

# Essential Practice Considerations

## Integration with Value-Based Care Enablement Strategy

As an organization considers its value-based care enablement strategy and goals, technology solutions should be an integral part of the analysis. Many VBC arrangements require participants to track and report on various data points including hospital readmissions, preventive care visits, and impacts to health outcomes. Successful VBC payment and quality arrangements require a unified exchange of data among a number of organizations, including labs, hospitals, imaging centers, pharmacies, and other providers and care team members. Technology plays an inescapable role in any organization's ability to reach their value-based care goals.

Without sufficient technology system(s), a participant in the value-based care world may find themselves at a disadvantage which could impact their performance. Thus, the need for participants to have technology systems that can meet the minimum reporting requirements of a VBC arrangement is becoming non-negotiable.

For example, participation in a clinically integrated network—often an early entry point into the VBC world—generally requires participants to have an EHR that meets minimum interoperability requirements. The lack of such a system could act as a significant barrier to an organization otherwise exploring its ability to participate in VBC arrangements. However, organizations looking to establish EHR systems can also benefit from cost savings.

## Intellectual Property

While there are numerous technological tools available to support a practice's VBC strategy, many benefit from or even require some level of customization. Some more enterprising organizations are regularly innovating internally, discovering new methods to improve care and lower costs, and may choose to employ or contract with engineers to bring these ideas to fruition. These efforts can be beneficial because they allow the practice to develop a product that is closely tailored to the practice's needs. However, internal product development can also present its own challenges.

It may be tempting to demand exclusive ownership of anything developed outside of pre-existing intellectual property (often called "background IP") when working with a vendor to implement, integrate, or customize a new tool. Before doing so, an organization should decide whether, and to what extent, they want to be in the business of owning, controlling, or licensing such intellectual property. For such vendors, their background IP, as well as the learnings gathered with or feedback obtained from each client, is core to growing their business—they are likely to resist forfeiting control. Adding to potential challenges to IP ownership, whether a creation is dependent on other intellectual property can trigger questions regarding derivative rights (discussed below). It is therefore important for organizations to establish with third parties how the ownership of intellectual property will be determined prior to its anticipated development.

## Rights to Evaluate

Unsurprisingly, practices often wish to try out a product in a real-world setting before committing to a long-term license, especially for "core" products like EHR systems that could seriously affect practice management functions. These tests, however, come with their own unique considerations and challenges.

Before allowing any integration or exposure to existing systems, parties often require an evaluation or testing period. This trial period can be defined as an "out" or early termination right in a larger multi-year agreement with a technology provider. It can also be covered by an entirely separate agreement specifying the trial or evaluation period, which would automatically terminate at the end of the trial period or if the provider enters into a longer-term arrangement. The agreement may also limit the product's access to certain sensitive practice functions and systems during this trial period. However, organizations should consider their exposure risks even in the limited window, particularly if the product requires access to practice data or systems to demonstrate its functionality. Customization and integration for testing purposes may require separate costs (either paid up-front or built into the longer-term agreement), and may raise issues related to confidentiality, privacy, and integrity of existing systems. Practices should carefully review the parameters of any proposed trial period to ensure it is sufficient to truly explore a tool's capabilities, and not overstep any of the vendor's intellectual property boundaries. Tool providers are also unlikely to provide robust warranties and will significantly limit their own liability during a trial period.

Practices may not always track the terms of their trial period and their transition to "full" access to the product. This can be challenging because the financial terms of the agreement may change (e.g., higher license fees may apply). The practice also may find it more difficult to exit the agreement after it transitions from a "trial period" to full participation. For these reasons, a practice may want to establish certain clear steps as part of the end of the trial period. These could include defining minimum levels of functionality and integration and requiring the product to meet certain evaluation metrics. The agreement may also require a certain number of education and training sessions before the organization formally accepts the longer-term arrangement. For new, complex, or feature-heavy technologies, a practice may also require continued education and training to maximize the benefits; any agreement should establish minimum frequencies and methodologies for such education.

## Cultural Fit

Effective evaluation of a technology is greater than simply vetting whether it does what it claims. The technology also needs to align with the practice's needs in order to succeed in their VBC arrangements. Multiple tools may exist to address the same challenge, but one size does not fit all. For example, there are hundreds of certified EHRs, each with different workflows, focuses, levels of efficiency, and features. For any technological innovation, finding the right fit also depends on an individual practice or organization's culture.

- *What is your current technological ecosystem? What are its capabilities for integration and compatibility? What is working for you, and what isn't?*

  To know if you are moving forward, you must first know where you stand. A practice cannot improve its technological capacity without careful assessment of its existing infrastructure, including current systems' scalability, what services or features are core needs versus "nice to have" benefits, if any elements are approaching end-of-life, compatibility with other systems or services (including those used by partners in VBC arrangements), how well the current system supports the practice's VBC strategy (for example, through data reporting and analytic functions), and data transfer capabilities. Integration between some systems may be difficult, costly, or simply not possible, and may eliminate some options if existing technology needs to be preserved. Practices should also evaluate existing contracts and termination rights, as well as key vendor relationships. Understanding the costs and benefits of existing systems and what may be necessary to replace them, a practice can explore what may be compatible with legacy technology, if the challenge of replacing it is worth the effort, or if certain relationships with other organizations are even feasible (see discussion about partnerships below).

- *What is your growth plan? What is your target technological ecosystem? What life-cycle does this next investment need to support?*

  Before moving forward, you should have a vision of where you are going. Some practices may simply be looking to update or modernize to a new status quo that will remain stable for a material time period. Others may have an aggressive growth plan. Still others may be aligning with another organization, such as an ACO or a local health system, which already has an established technology ecosystem. Knowing not only how but at what pace an organization intends to develop, evolve, or integrate should factor into technology acquisitions. A smaller investment may be necessary to get through a growing phase, greater investment up front may help drive a practice toward its goals, or a major investment may be mandatory as a condition of joining other providers in a new VBC opportunity. Some organizations may determine that third-party technological solutions are insufficient, or do not encompass their original idea. An organization may want to bring engineers in-house or partner with a technology development entity to develop a custom or semi-custom solution.

- *How tech savvy is your organization overall? What are the different strata of technology in your practice, and the sophistication within each? Do you have the people power (quality and quantity) to effectuate the level of technological innovation you hope to achieve short term? Long term?*

  Every organization has a unique level of sophistication when it comes to technology generally, as well as for individual specialties. Taking a massive leap in system sophistication or complexity is not impossible, but it may be ill-advised if proper groundwork is not laid for such a shift. For example, an ophthalmology practice may have utilized the same basic, but older EMR system for a decade, while also being well-versed in highly sophisticated medical equipment. For this practice, incorporating cutting edge AI tools into diabetic retinopathy workstreams may be simple, but converting to the newest and largest EHR without a long-

term training and education plan, as well as strategic buy-in from all members, could be a painful (and pricey) undertaking. An organization must also have the ability to support transformation. A practice must assess its internal capacity, and whether it has an information systems team capable of onboarding, maintaining, and maximizing the capabilities of any technology. A practice can also consider contracting with a managed service provider to help handle its information technology needs, but such relationships require their own careful scrutiny and planning. Note that ACOs and other participants in VBC programs may have more legal flexibility to provide personnel or services to support this kind of significant technological change.

- *What is the size of your practice? What is the scale of the problem you hope to rectify or benefit you wish to achieve through this particular technological investment? Does the expenditure align with the impact?*

  The right technology solution should match the size of the problem and the goals of the practice. The best technology for a particular challenge in a VBC arrangement may not necessarily be the most intricate, advanced, specialized, or customizable. An organization should not be spending money on bells and whistles it will never (or rarely) use. Some efficiencies or benefits may also not have a material impact or savings at a smaller scale. However, some technological systems are better at growing with a practice than others, which may be more cost effective than having to integrate other existing technologies or developing custom solutions.

**Key consideration**

Software as a service ("SaaS") is the most common form of software delivery model. Instead of providing software on a physical resource like a CD, it is a cloud computing service model, where the software is hosted by a third-party provider and (most often) accessed via a web application. Typically, instead of a one-time transfer of ownership, SaaS products are paid for based on a subscription or license fee. For example, many EHR products are SaaS models, in which practices receive a defined set of features accessed via a web portal in exchange for a monthly or yearly license fee. The "as a service" model has now expanded to features other than software (as described elsewhere in this document).

## Alignment with Future Strategic Direction of the Organization

Prior to embarking on the process to integrate value-based care technology solutions into your organization, thought and consideration should be given to the future direction of the organization. Implementing a new technology solution is a serious undertaking from financial, administrative, and integration perspectives. Often, such endeavors constitute capital projects requiring long-term budget planning. Careful thought should be given to the lifespan of any new technology tools to determine whether a return on investment is feasible.

**Questions to ask include:**

- Is the technological investment tied to a particular revenue opportunity, like a governmental value-based model?
- Examine your organization's owners; are individuals nearing retirement?
- Is there an appetite to seek out or improve your technology capabilities?
- Financials aside, making a significant investment in your technology system can be disruptive to your operations. Is your organization prepared to work through the inevitable growing pains associated with new technology?
- Do you have the opportunity to work with partners like enablement entities, health systems, or ACOs that can shoulder some of the costs (and are you comfortable with the terms of any such relationship)?

In an era where value-based care is becoming the rule, not the exception, potential partnerships with other organizations with the technology capabilities required to navigate these novel payment arrangements can be a fruitful strategy—particularly if considering bringing in additional owners or selling the organization. By increasing the technological capabilities of the organization, it may be better positioned to participate in VBC arrangements.

## Payment Opportunities

Some technology solutions present direct or indirect payment opportunities. For example, remote physiological monitoring solutions and care management services (discussed above) may be billable services under Medicare and other payers in some cases. As a result, investment in these technologies may allow a practice to advance the overall quality and cost goals of a value-based care arrangement (for example, by reducing hospital readmissions), while simultaneously rendering a billable service. Additional information about digital medicine coding is available here.

Similarly, payer sponsors of VBC arrangements may support certain technological investments as part of the payer's overall administrative goals. For example, payers sometimes cover some or all the costs of implementing an electronic visit verification ("**EVV**") system for home-based services, which allow clinicians to utilize a smartphone or tablet to electronically verify patient home visits. Payers invest in this technology because it is easier to validate and promotes goals of reducing waste and fraud. The result is that there is no hardware cost to the practice, and the clinician is able to bill for their services in compliance with EVV requirements.

# Negotiating Technology Agreements

Once an organization's technology needs are identified, the next step is to select a vendor and enter into an agreement for the products and/or services. Many practices start with informal information collection through colleagues, medical organizations, specialty societies, and partners in their value-based arrangements to identify vendors and to obtain firsthand accounts of peer experiences. Practices then usually move on to more formal steps.

## Identifying Prospective Vendors/Solutions

If administrative bandwidth allows, consider issuing a request for information ("**RFI**") and/or a request for proposal ("**RFP**"). An RFI is a preliminary step in the procurement process aimed at obtaining high-level information from vendors to help whittle down the pool of prospective choices. RFPs are more detailed and are intended to solicit bids from vendors for price and service comparison. HealthIT.Gov offers several resources to assist with vendor evaluation.[10] For an RFI and RFP to be successful, the practice will need to develop a detailed understanding of its existing IT systems and technology needs to meaningfully evaluate vendor responses.

### Key consideration

An RFI or RFP usually is not required by law or regulation (except for certain government-sponsored arrangements). Instead, this is simply a common way to ensure the practice is working with a vendor that meets its needs in terms of expertise, capabilities, and cost.

## Types of Technology Agreements

Once a vendor is selected, practices should carefully review the agreements structuring the affiliation. There are several types of health care technology contracts, and they will vary in importance and complexity depending on the nature of the relationship and products involved. While the following contract types can be combined in an endless number of variations, at a high-level, they include:

- *Services Agreements:* Under this type of agreement, the vendor will provide certain identified services; e.g., help desk services, hardware maintenance services, data export/import services.
- *Software Agreements:* This agreement details the purchase, license, or other accessibility to a software product, whether installed locally or accessed remotely via the cloud. Modern software agreements are usually structured as SaaS arrangements (defined above).
- *Hardware Agreements:* Also sometimes called *Hardware as a Service* ("**HaaS**"), a vendor is selling, leasing, or otherwise providing hardware such as servers, computers, or specialized medical equipment with technology interfaces.
- *Cloud Agreements:* Under this type of agreement, the vendor provides access to software and other solutions, like serverless computing, remotely via the cloud. This type of agreement may also be called *Infrastructure as a Service* ("**IaaS**") or *Platform as a Service* ("**PaaS**").
- *Data-Related Agreements:* These agreements typically authorize the sharing, access, and ownership of a party's data. They can include data use agreements ("**DUAs**") and business associate agreements ("**BAAs**"), among others.

## Technology-Specific Contract Considerations

Practices can prepare effectively for vendor contract negotiations by being aware of several issues specific to health care IT solution arrangements.

- *What are you actually buying?*

  Due to the intangible nature of many technology solutions, you should understand the nature of what is being acquired. While this is easier to understand in the context of hardware (for example, "you are buying ten desktop computers"), it is less clear in service, software, and cloud contexts. Often, entering into a technology agreement means you are receiving a license to the product. A license is an authorization granted by the vendor/developer/manufacturer to you that dictates how end users can access and use the product. Licenses may be limited in purpose (i.e., a license to use a product for personal use only), limited by user (i.e., a license for physician use only), and/or limited in duration (i.e., a license to access a product during the contract versus a lifetime license). Several licensing models exist; ensure you have a clear understanding of the nature of the license you are acquiring. Also, make sure you understand which entity holds the primary license – if your license is secondary or subject to another entity (such as a health system sponsor), you may have less ability to customize your use of the product. Finally, understand the full bundle of items and services you will receive – hardware, software (including any specific features or add-ons), upgrades and ongoing maintenance, and services (such as customer support and training).

- *What is this going to fully cost?*

  Many vendor agreements include an implementation fee, a licensing fee (usually tied to the total number of authorized users), as well as support fees and training fees. Outside these preliminary costs, consider your possible future costs:

  1. If your organization gains or loses locations/users, will the cost increase/decrease?
  2. If additional products may be required at a later time, what will they cost and can that cost be agreed upon upfront?
  3. How long is the warranty and maintenance period?
  4. Is support included?
  5. Are future maintenance costs ascertainable?
  6. Are there penalties or other fees if you fail to reach a minimum utilization threshold?
  7. Is there a cap on price increases?
  8. Are the pricing terms tied to your participation in a value-based arrangement or work with a particular enablement entity so that, if the arrangement ends, the financial terms change?

- *How long is this going to take?*

  Depending on your existing systems and the nature of the solution purchased, you can expect several weeks to months to pass before your project is complete. As with any long-term endeavor, delays and setbacks are possible. It is important to set forth an implementation plan in your technology agreements. **Implementation** refers to the process of making a new technology, system, or software operational within an organization. It encompasses a range of activities, including installation, configuration, customization, testing, user training, and ongoing support. By identifying each phase of implementation and assigning timelines for their completion, you can ensure your project remains on-track. Contemplate tying installment payments to certain implementation milestones. You can also consider negotiating incentives if the vendor adheres to the implementation schedule. For example, an agreement might specify an anticipated five-year timeline, with incentives for achieving certain milestones each year.

- *Can you evaluate the technology?*

  Before signing a contract, determine whether the vendor has a testing environment available for your evaluation. Similarly, connecting with peers who utilize the solution may provide an opportunity to evaluate the solution before committing. Once signed, moving from contract execution to go-live can present a number of functionality and operational issues like downtime, outages, and other problems; these can be particularly debilitating for health care organizations. **Acceptance testing** is a key issue to consider during negotiations. Acceptance testing means verifying the final product meets specified business requirements and user needs. It involves validating functionality, performance, and usability to confirm the product is ready for deployment. Your agreement should allow you adequate time to perform acceptance testing as well as a process and timeline for the vendor to correct any issues detected during testing.

- *Is your data safe/secure?*

  Top of mind for most health care providers researching technology solutions is data privacy and security. There are several state and federal laws that protect the types of data stored by health care organizations, including HIPAA (additional HIPAA considerations discussed in detail below). Notably, there are other types of protected data that your organization may store/access, including personal identifying information and payment card information that merit consideration. The repercussions for failing to safeguard such protected data are significant. When evaluating a vendor and a technology contract, ensuring your data will be protected is paramount. Determine whether the vendor storing, transmitting, and/or accessing your data from non-U.S. locations (also known as offshoring). Identify whether the vendor is required to encrypt or otherwise secure data in their possession. Is the vendor authorized to use your data, whether directly or indirectly, for their own purposes, i.e., to train augmented intelligence models? Who owns the rights to information derived from your data?

- *What liability are you incurring?*

  Entering into a technology solution contract could open up your organization to potential liability in a variety of ways. Intellectual property infringement is a potential risk in technology agreements, including liability alleged by third parties whose products are used by your vendor; ensure your vendor appropriately indemnifies your organization against such claims. Requiring adequate insurance coverage can be critical to minimizing your liability exposure. In addition to your standard policy requirements, you should require all technology vendors to provide adequate cyber liability coverage. Depending on the size of

your organization, it is not uncommon to require policy limits exceeding five million dollars. If you are receiving access to a technological tool through a value-based care partner, ensure that you understand your exposure and rights under such agreements. For example, does the indemnification cover your practice and users? Can your practice independently demand indemnification even if the ACO, health system, or other partner does not?

- *What happens when you move on from a technology solution?*

  Advance planning in terms of a post-termination transition is vital. In particular, it is essential for your organization to determine the procedures for transitioning your files, data, and proprietary information to a new solution. It is imperative to ensure the vendor is not permitted to hold your data hostage (i.e., preventing you from accessing your own data) upon termination/expiration of the agreement. Consider addressing transition services in the agreement. Are you required to return any hardware that was provided by the vendor? Will you have to pay any termination fees or other penalties to end the contract early?

This list reflects common considerations that may inform practices going into vendor negotiations. However, technology arrangements potentially raise many more issues depending on the nature of the technology, the financial arrangement, and the parties. Practices should consider engaging competent legal counsel to protect the organization's interests and to be certain a prospective arrangement complies with all applicable state and federal laws.

# Collection and Use of Data

Outcome-optimized care requires a significant volume and variety of data. Much of the data comes from payers and fellow participants in VBC plans. Aggregating and analyzing that data has the potential to surface new insights and areas of improvement in patient care, prevention, administration, and beyond.[11] Efforts to improve population health often require a holistic approach to data collection, including medical histories, health status and treatment monitoring, and social contributors to health data. Such a rich well of data is highly valuable and sought after for a multitude of other technological purposes and innovations; it is also often highly personal and tightly regulated. Patients grant health care providers access to sensitive data for particular purposes, and the law requires them to safeguard that trust.

Despite its powerful potential for good, it is important to recognize the real potential for abuse of such data and the ethical implications of using a patient's data without their consent. HIPAA reflects that organizations are the guardians of such data—covered entities as defined by HIPAA[12] must protect the privacy and security of health information, and contractually obligate their business associates to do the same.

Third party technological solutions often require the use or disclosure of PHI to perform their delegated services on a covered entity's behalf. Organizations must pay close attention to what they may contractually authorize that third-party to do with the data they share, both on behalf of the organization and on behalf of the third-party.

**Other data privacy laws**

While HIPAA is the most commonly cited federal health care privacy law, practices should be aware of other applicable rules. For example, the Federal Trade Commission's Health Breach Notification Rule applies to health data that may not be PHI, and many states have adopted health privacy laws or comprehensive privacy laws.

## Services Related to Improving or Refining a Tool

For any relationship that requires a BAA with the vendor, practices should use extreme caution if their vendor agreements allow use of practice data to improve vendor offerings. Third-party technology developers and vendors, particularly those unfamiliar with the health care regulatory space, often attempt to claim expansive rights to use PHI for their own research and development after gaining access as a business associate. Their interests may even align with an organization through continued improvements or refinements to the relevant technology. Nevertheless, practices should be cautious about the uses they authorize because such uses may violate the law.

Under HIPAA, a covered entity (like a physician practice) may allow a business associate to create, receive, maintain, or transmit PHI on its behalf. That access is not an unfettered license for the business associate to use PHI as it pleases. Generally, a business associate can only use PHI in ways that would be permitted for a covered entity. HIPAA also requires that a technology vendor may only use PHI as contractually directed by the covered entity. Most transfers of PHI in the value-based care context fall under the category of "healthcare operations;" if so, the organization and vendor must utilize the minimum necessary PHI to perform the specified business function.[13] This rule often tightly limits vendors' access to data, unless such data is deidentified or otherwise meets a HIPAA exception.

## Prohibition on the Sale of PHI

In addition, the sale of PHI is expressly prohibited unless authorized by the patient.[14] A **sale** is described broadly, including where anything of value is directly or indirectly received from or on behalf of the recipient of the PHI. This may include practices like providing a discount if the practice permits access to PHI or retaining PHI to improve, refine, or train a system. A practice may be at higher risk if the reasons for transferring PHI are vague or unclear. Practices can manage this risk by considering whether the arrangement clearly defines the services, the use case for the PHI, and how they are permitted by the organization. If a vendor wants to improve or refine a tool for use beyond its immediate clinical benefit, the terms must be structured carefully to avoid slipping into a violation for both the vendor and the practice.

## Managing Cybersecurity Risk

When selecting a tool or working with a vendor, privacy and security compliance go hand in hand. Practices should assess a new technology's ability to integrate with its existing HIPAA privacy and security measures. They should also evaluate the security capabilities within the tool if needed, such as encryption and access controls, and review any history of previous security incidents, weaknesses, or failures.

**Key consideration**

When considering a potential business associate, organizations must go beyond just the tool to the vendor itself. What are the vendor's physical, administrative, and technical safeguards to protect PHI? Do they have HIPAA-related policies and procedures? Who is their privacy officer? Has the vendor had previous security incidents or data breaches, and if so, how were they handled? What are the vendor's disaster recovery and backup plans?

# Compliance Considerations

As with nearly every undertaking in healthcare, ensuring your organization maintains compliance with applicable state and federal laws and regulations is of utmost importance. Incorporating technology solutions into an organization participating in a VBC arrangement can present some unique compliance considerations.

## Professional Liability

As technology becomes more sophisticated, there may be a tendency to delegate traditional clinical tasks to outside tools. But technology is not a substitute for the knowledge, education, and experience physicians and other practitioners bring to bear. In most cases, as a legal matter, the treating physician or practitioner maintains overall responsibility for the quality of patient care.

This can create a challenge in VBC arrangements, which frequently require physicians to adopt a uniform set of technological tools. These tools may be attractive for the reasons described in this document, but physicians should remember that they may remain personally liable for errors caused by these tools. There is a mismatch in incentives; value-based care may provide "upside" financial incentives for managing a population's care, but allegations of malpractice (or similar professional liability) are usually directed to a single physician. Practices can guard against these risks by ensuring any agreements with ACOs (or similar value-based care entities) and any clinical protocols related to technological solutions preserve their ability to make independent medical judgements.

## Physician Investment in Technology Companies

Given the great opportunities for technological innovation in health care, it's no surprise that physicians often wish to invest in companies offering these tools. However, physicians should be aware of fraud and abuse risks in such investments. At a high level, the federal Anti-Kickback Statute ("**AKS**"), Physician Self-Referral Law ("**Stark Law**"), and False Claims Act each regulate certain kinds of physician investments.

In particular, the HHS Office of Inspector General ("**OIG**") has raised concerns that physician ownership in entities to which they refer may implicate the AKS, which prohibits the offering, solicitation, or receipt of anything of value if intended to refer or otherwise generate federal health care program business. Although the OIG did not prohibit such physician investments, it set out important guidelines for physicians to assess whether these investments may be abusive. For example, under OIG guidance, arrangements are more suspect if physicians do not make bona fide capital investments, if they receive returns out of proportion to their investment, or if they receive investment opportunities based on their actual or potential business generated for the entity.

Similarly, the Stark Law fully prohibits physician ownership in entities that furnish or bill for certain kinds of "designated health services" (including certain medical devices) paid under Medicare. Physicians should carefully evaluate the terms of any financial relationship with a technology company to ensure it complies with the law.

## Paying for Technology Tools

Value-based care arrangements often involve entities like ACOs or health systems helping practices implement better (or at least different) forms of technology. These are financial relationships that must be evaluated under the AKS, Stark Law, and potentially other laws. Both the AKS and Stark Law have provisions allowing the donation of electronic health record technology, but these place restrictions on the type of technology provided and may not cover all necessary practice investments in hardware and services related to implementation and ongoing operation. Both laws also include flexibilities for certain relationships involving "value-based enterprises," but these flexibilities can be complex to establish and have important limits. For example, they may be limited to certain kinds of items and services, or they may require individual providers to take on risk. Finally, some federal government VBC models, including the MSSP, have established waivers of these laws for financial relationships reasonably related to the purposes of the MSSP and distributions of MSSP shared savings.

### What qualifies as a value-based enterprise?

A "value-based enterprise" (VBE) is defined in the Anti-Kickback Statute regulations as two or more "VBE participants" collaborating to achieve at least one "value-based purpose," each of which is a party to a "value-based arrangement" with at least one other participant in the VBE; that have an accountable body or person responsible for financial and operational oversight of the value-based enterprise; and that have a governing document that describes the value-based enterprise and how the VBE participants intend to achieve its value-based purpose(s). A VBE does *not* necessarily need to be a separate legal entity, as long as it meets these standards.

Practices participating in value-based care arrangements may also provide certain kinds of technology to their patients. These may include formally prescribed beneficiary supports (like SaMD tools that may qualify as remote patient monitoring) as well as other supportive technologies to help patients achieve their care goals (such as electronic scales or self-management apps). Although the AKS and other HHS rules generally prohibit an entity from giving a beneficiary anything of value if it is likely to influence their choice of provider, there are several exceptions to this rule. For example, practices are allowed to provide transportation in some cases, as well as certain non-abusive items to promote access to care or adherence to a treatment regimen.[15] ACOs in the MSSP, and certain other governmental VBC models, give practices added flexibility to provide valuable items to beneficiaries, including technological tools for self-management of conditions. Finally, MA plans and commercial plans may offer supplemental benefits that go beyond traditional clinical care, including nutritional assistance, gym memberships, or potentially even housing assistance.

# Conclusion

Technology can be a key component of a successful transition from a volume-based payment arrangement (i.e., FFS) to a holistic care model based on value (i.e., VBC). However, practices should be thoughtful about their options and consider possible business and legal risks as they evaluate strategic alternatives. Practices can maximize their chances of success by developing a clear picture of their existing capabilities, gaps or needs that must be addressed by any technological tool, and value-based care strategies.

# References


1 Atherton J. Development of the electronic health record. *AMA J Ethics.* 2011;13(3):186-189. https://journalofethics.ama-assn.org/article/development-electronic-health-record/2011-03

2 HITECH Act of 2009, 42 USC sec 139w-4(0)(2) (February 2009), sec 13301, subtitle B: Incentives for the Use of Health Information Technology

3 Office of the National Coordinator for Health Information Technology (ONC). *Office-Based Physician Electronic Health Record Adoption*. Health IT Quick-Stat #50. Published October 2023. https://www.healthit.gov/data/quickstats/office-based-physician-electronic-health-record-adoption

4 *See* 85 FR 25642 (2020), 42 C.F.R. § 170.315(g)(10); 170.404.

5 US Food and Drug Administration. *Software as a Medical Device (SaMD)*. Digital Health Center of Excellence. https://www.fda.gov/medical-devices/digital-health-center-excellence/software-medical-device-samd

6 Medical Group Management Association. *Leveraging Value-Based Care Data Analytics to Improve Outcomes*. Published 2022. https://www.mgma.com/articles/leveraging-value-based-care-data-analytics-to-improve-outcomes

7 American Medical Association. *Augmented Intelligence Development, Deployment, and Use in Health Care*. Published November 2024. https://www.ama-assn.org/system/files/ama-ai-principles.pdf

8 Federal Trade Commission. *FTC Announces Crackdown on Deceptive AI Claims, Schemes*. Published September 2024. https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes

9 See American Medical Association. *Augmented Intelligence in Health Care*. AMA Policy H-480.940; *Augmented Intelligence in Health Care*. AMA Policy H-480.939; *Use of Augmented Intelligence for Prior Authorization*. AMA Policy D-480.956.

10 US Assistant Secretary for Technology Policy. *Vendor Evaluation Matrix Tool*. Office of the National Coordinator for Health Information Technology. https://www.healthit.gov/resource/vendor-evaluation-matrix-tool; *Vendor Meaningful Use Compare Tool.* Office of the National Coordinator for Health Information Technology. https://www.healthit.gov/resource/vendor-meaningful-use-compare-tool; *Vendor* https://www.healthit.gov/resource/vendor-pricing-template

[11] American Medical Association; AHIP; National Association of ACOs. *The Future of Sustainable Value-Based Payment: Voluntary Best Practices to Advance Data Sharing*. Published 2023. https://www.ama-assn.org/system/files/data-sharing-playbook.pdf

[12] 45 CFR § 160.103

[13] 42 C.F.R. § 164.502.

[14] 42 C.F.R. § 164.502(a)(5)(ii).

[15] *See* 85 FR 77684, 77797 (Dec 3, 2020)

**Disclaimer**

The information and guidance provided in this guide are believed to be current and accurate at the time of posting. This document is for informational purposes only, and the information and guidance contained in this document are not intended and should not be construed to be or relied upon as legal, financial, medical, or consulting advice. It is not intended as a substitute for the advice of an attorney or other financial or consulting professional. Each health care organization is unique and will need to consider its particular circumstances and requirements, which cannot be contemplated or addressed in this guide. References and links to third parties do not constitute an endorsement, sponsorship, or warranty by the American Medical Association, and the AMA hereby disclaims all express and implied warranties of any kind.