E-Briefings

Volume 14, No. 6, November 2017

Welcome to The Governance Institute's E-Briefings!

This newsletter is designed to inform you about new research and expert opinions in the area of hospital and health system governance, as well as to update you on services and events at The Governance Institute.

In this issue:

Governance Impact: Evaluating the Future of Bundled Payment Models

By Mark E. Hiller, M.B.A., and Guy M. Masters, M.P.A.

On August 15, 2017 the Centers for Medicare & Medicaid Services (CMS) proposed cancelling the mandatory Episode Payment Model (EPM) bundles for the following areas:

- Acute Myocardial Infarction (AMI)
- Coronary Artery Bypass Graft (CABG)
- Surgical Hip and Femur Fracture Treatment (SHFFT)
- Cardiac Rehabilitation Incentive Payment Model

The primary objective of the proposed cancellation is to eliminate further mandatory expansion of these programs, largely due to stakeholder concerns about large-scale mandatory models. It is important to note that while CMS also proposed changes to the Comprehensive Care for Joint Replacement (CJR) model, it did not cancel CJR or any of the changes to CJR that were published in the previous EPM final rule. Comments on the ruling were due to CMS by October 15, 2017.[1]

[1] Premier's Comments on the EPM Cancellation CJR Changes Proposed Rule, Premier, Inc., October 16, 2017, https://www.premierinc.com/wpdm-package/premiers-comments-epm-cancellation-cjr-changes-proposed-rule/.

Is CMS Giving Up on Bundled Payment Models?

CMS is not giving up on bundled payment models, however what they have proposed is merely rolling back the expansion of "mandatory" participation. It was no secret that the former Secretary of Health and Human Services, Tom Price, M.D., was against mandatory bundled payment participation for providers but he was still supportive of voluntary initiatives. With Dr. Price's departure, the stance of CMS on the future use of mandatory models is not clear. However, voluntary programs have been supported for many years by both CMS and healthcare providers. In fact, CMS is expected to announce a new voluntary bundled payment program in the near future. It is in the best interest of the industry to continue these programs as voluntary models in addition to those that already exist.

Current Status

CMS has four existing bundled payment programs:

1. The voluntary Bundled Payment for Care Improvement (BPCI) program: This program was officially announced in 2011 and went live in October 2013. It will end in September of 2018. This program is the largest Medicare bundled

payment model with 48 conditions (correlated to approximately 180 MS-DRG codes). This model includes broad participation by hospitals, physician groups, and post-acute providers. CMS is expected to replace BPCI in 2018 with a new voluntary program, tentatively being referred to as BPCI-Advanced (BPCI-A). The anticipated BPCI-A model is explained further in this discussion.

2. The voluntary Oncology Care Model (OCM): This model went live in July 2016 and is comprised of approximately 200 oncology groups (note that this is not a hospital model).
3. Mandatory CJR: This model went live in April 2016 and is comprised of approximately 800 participating hospitals.
4. Mandatory EPM model: Mandated bundles for CABG, AMI, and hip and femur fractures. This is the model that CMS has proposed to cancel.

Board Strategy Considerations

For hospitals and health systems in an existing CJR mandatory market, the EPM rule change, if adopted, will make approximately half of these markets voluntary effective January 1, 2018. Recent results from the first two quarters of the CJR program show that nearly half of participants received gainsharing payments for meeting cost and quality performance goals. It is encouraging to see this model generating results so early on. Current bundled payment participants in voluntary markets should take the opportunity to evaluate the potential risks and rewards of continued CJR participation.

Considerations should include the following:

- CJR quantitative and qualitative results to date, and the effects of program design changes on future CJR success.
- The potential effect on further alignment opportunities with physicians and other providers through gainsharing and Advanced Alternative Payment Model (APM) qualification under MACRA.
- Impacts on care delivery, quality, and patient experience.
- Implications on competitive position in the market.
- The potential effects on participation in the expected BPCI-A program.

Bonus: MACRA Payment Increase through AAPM Status

Under the previously finalized EPM final rule, an important change to CJR is the creation of two tracks within the program. One track will potentially qualify providers as participants in an Advanced APM under MACRA guidelines and the other track would not. The track that enables providers to obtain Advanced APM status through the CJR program will potentially qualify participating clinicians to become eligible for the annual five percent Advanced APM Incentive Payment beginning in January 2019.

As MACRA's Quality Payment Program (QPP), which was passed by a Republican Congress, continues to move forward, bundled payment models create an opportunity to engage with providers—especially specialists—across many different clinical categories. We already see this occurring across the country with the 48 conditions in the existing BPCI program and a continuation of this broad opportunity once BPCI-A is announced. Therefore, these models not only represent a smart business choice for providers to ensure continued economic viability in today's value-based healthcare environment but also help to retain top talent as physicians are attracted to Advanced APM programs.

Assess the Value of BPCI-A Participation

Regardless of whether an organization has or has not participated in a bundled payment model to date, it is important to evaluate the opportunities BPCI-A could provide. At a minimum, obtaining the claims data that CMS typically makes available with the launch of this type of program will provide valuable insights as to where patients are going for care, what services they are accessing, the cost to Medicare to provide these services, and potential opportunities for improved alignment across services.

Other benefits and impacts to consider include:

- Competitive advantage and provider/physician alignment go hand in hand: Thousands of providers are already participating in bundled payment models, learning how to manage patient

care across the continuum, and getting paid for their successes.
    - *Gain experience.* Bundled payment participation increases an organization's experience with transitioning to value-based payment models and managing increasing levels of financial risk.
    - *Avoid being last to the game.* Historically, providers that have elected to engage in these models earlier than others have positioned themselves to have precedence over providers that joined later. Additionally, a system with significant hospital assets needs to consider that Medicare has in the past placed a priority on physicians in these models and gives them precedence over hospitals when it comes to who CMS ultimately attributes the bundle savings (and financial risk). Further, due to the prevalence of many provider types (e.g., physician groups, post-acute providers) and the precedence issue, there is heightened competition between independent provider types and also between systems competing for the independent providers.
    - *Retain top talent.* Participation in a bundled payment model is especially important to think about in a market where competitors are participating in these models to avoid losing top talent. Engaging independent providers early on is essential, as others will likely be knocking on their door and many are already aligned with third parties. However, providers may be able to create an offer that makes them rethink their current alignment. Achieving alignment with Advanced APM status is essential to gain additional financial incentives, if requirements are met, as well as to attract high-value physicians.
- Financial upside potential: Bundles allow a unique opportunity to potentially earn more than 100 percent of Medicare reimbursement. Participation in multiple successful bundles can multiply this potential "more than Medicare" opportunity.
- Quality improvement and cost efficiencies: Use bundles as an opportunity to improve care delivery, enhance patient experience, receive generated savings, and create models to share those savings to align independent providers with systems.
- Commercial payer alignment: Providers achieving success in CMS bundled payment programs can leverage their care delivery improvements by negotiating new payment strategies with commercial payers that are already benefiting from the bundle due to better patient outcomes and lower costs. Commercial payers now make up the majority of covered lives for alternative payment arrangements, so it is important that providers participating in these models seek out and partner with them to achieve additional financial success.

Risks and Mitigation

Typically an organization's bundled payment performance in the first year doesn't include downside risk. In the second year and beyond, providers will be exposed to varying levels of financial risk (meaning potential episode cost overruns would need to be paid back to CMS), which are capped at an increasing limit over time. Typically these models include stop-loss provisions (e.g., caps at the individual episode level) to also limit financial losses. In the worst case, the new programs (similar to the existing BPCI provisions) will likely have a provision for being able to drop out of the program if long-term success is not viable.

In the Boardroom: Opportunities and Perspective

Bundles are far from dead. They are still seen as a key component in the movement toward value-based payment and population health management. The proposed cancellation of portions of the EPM rule this past August was focused on stopping the push by the previous administration to roll out mandatory bundles. There is no question that Congress, CMS, and even commercial payers are moving providers to upside and downside financial risk-based payment models.

The expected new BPCI-A program will create significant opportunities in many areas such as:

- Claims data availability: Get the data. It's an opportunity to receive significantly

valuable information on where patients are going, enabling your organization to look for and analyze opportunities for care improvement and savings.
- Financial upside: Get paid your normal Medicare amount and potentially receive bonus payments on top.
- Provider incentives: Any savings generated can be used to incent alignment across multiple providers to improve cross continuum care delivery and increase focus on the patient.
- Value-based payment: Participation will allow you to learn or enhance your knowledge and expertise in how to align and integrate with providers to manage risk across the continuum.

Take advantage of the opportunity to evaluate if bundled payment models are appropriate for your organization, community, patients, and providers. Explore the potential for your organization to use bundled payment models to improve the quality of care, strengthen provider alignment, retain top physician talent, and increase margins at the same time. Thousands of providers already are.

The Governance Institute thanks Mark E. Hiller, M.B.A., Vice President-Engagement & Delivery, Premier, Inc., and Guy M. Masters, M.P.A., Principal, Premier, Inc., and Governance Institute Advisor, for contributing this article. They can be reached at mark_hiller@premierinc.com and guy_masters@premierinc.com.

■■■

Myths and Fallacies of Computer Security in Healthcare Environments

By Sean Peisert, Ph.D., Lawrence Berkeley National Laboratory

This article is an excerpt from The Governance Institute's December 2017 BoardRoom Press *Special Section. The full article will be available in December at www.governanceinstitute.com/TGIBoardRoomPress.*

The U.K. National Health Service (NHS), U.S. Office of Personnel Management (OPM), Experian, Sony, the Democratic National Committee, the Republican National Committee, the U.S. Department of Health and Human Services, Yahoo, Anthem, Premera Blue Cross, 21st Century Oncology, Banner Health. Anyone reading this probably recognizes each of these organizations as a few of the of dozens that have reported a cyber attack in recent years, such as ransomware or a database breach, and a few of the hundreds or thousands that have been the victim of damaging attacks but did not report it, and/or had one but failed to find one.

But why should I worry about security? Why would attackers target my organization? There are at least two answers: first, not all attacks are targeted. Malware can spread across the Internet and via devices such as USB sticks indiscriminately, and collateral damage can be high. Second, much like the proverbial story about the way to survive an encounter with a bear or shark being merely the ability to swim or run faster than the other people you're with, attackers may target your organization simply because you've made it easy for them.

Mitigation

Organizations looking to deploy more secure systems expect that attacks can and will occur. They develop systems that regularly identify the most valuable assets in the organization and potentially weak entry points, and assume that any system can and will be breached. In addition, organizations must regularly have scenario planning and exercises to identify what could happen in the event of a breach, and what actions can be taken to minimize damage and restore the system.

To that end, it should come as little surprise that security experts are finding that endpoints such as those based on Apple's iOS or Google's Chrome OS are often more

secure[2] than endpoints running traditional desktop operating systems, such as Microsoft's Windows. Tim Cook, the CEO of Apple, has indicated that an iPad, not a Mac, is his primary work machine.[3] How many people who live in Microsoft Word, Excel, PowerPoint, and Outlook could instead do just fine with Chrome OS?[4] How many people who are doing primarily Internet research could similarly use a Chrome OS device or iPad? A question from the board to your organization's Chief Information Officer might be: could some of our workers complete their tasks using more secure devices such as those that run on Apple's iOS or Google's Chrome OS?

The answer to security training is similarly nuanced. Security training of employees *can* improve results.[5] However, "beyond a certain threshold, increasing demands [on users] are simply met with attempts to circumvent onerous procedures. The thresholds appear to have been long exceeded for most users."[6]

This critique is not to say that conventional wisdom should be stopped immediately. But at the same time, it is important to note that merely following the herd by using so-called "best practices" is no longer defensible. In addition, it is vital for board members to understand that "compliance" with regulations (e.g., HIPAA and HITECH) is *not* the same thing as true "security." Computer security is about defending against active and well-financed adversaries. Running a computer in a public environment today means the weather is *always* snow with a chance of tornados, and the roads are *always* covered in black ice.

Alternative Approaches

Don't Go It Alone

There is at least one truism for many organizations struggling to find a path forward: for most organizations, unless you are Google, Facebook, Microsoft, or Apple, or unless you are a major medical center with a very large IT budget and are located in a city rich with computer security talent, you probably should not try to solve the problem on your own. Organizations such as these are familiar with the HITRUST CSF[7] inside and out, and have large security programs with elements such as strong, multi-factor authentication, system hardening, backups, meaningful and appropriate training, and real-time network and system visibility. Incident response and recovery are well understood and integrated into the environment. These organizations probably already identified whether they need to run their own storage and email systems, and if each of their personnel needs a full system running Windows, or whether Google Apps and Chromebooks will do.[8] If this describes your organization, you have a massive head start on doing "all the right things."

---

[2] Rich Mogull, "Tidal Forces: The Trends Tearing Apart Security As We Know It," January 3, 2017 (https://securosis.com/blog/tidal-forces-the-trends-tearing-apart-security-as-we-know-it); and Rich Mogull, "Tidal Forces: Endpoints Are Different—More Secure, and Less Open," January 18, 2017 (https://securosis.com/blog/tidal-forces-endpoints-are-different-more-secure-and-less-open).

[3] Jake Smith, "Tim Cook: 80 percent to 90 percent of my time is spent on an iPad, working and consuming," *9to5Mac*, February 14, 2012; Adrian Weckler, "Tim Cook: Apple won't create 'converged' MacBook and iPad," *Independent.ie*, November 15, 2015 (www.independent.ie/business/technology/tim-cook-apple-wont-create-converged-macbook-and-ipad-34201986.html).

[4] Google Chromebooks (www.google.com/chromebook/).

[5] Iacovos Kirlappos and M. Angela Sasse, "Security education against phishing: A modest proposal for a major rethink," *IEEE Security & Privacy*, Vo. 10, No. 2 (2012), pp. 24–32.

[6] Adam Beautement, M. Angela Sasse, and Mike Wonham, "The Compliance Budget: Managing Security Behavior in Organizations," *Proceedings of the 2008 New Security Paradigms Workshop (NSPW)*, September 2008, pp. 47–58; and Cormac Herley, "More is Not the Answer," *IEEE Security & Privacy*, Vol. 12, No. 1, 2014.

[7] HITRUST CSF v8, June 2016 (https://hitrustalliance.net/hitrust-csf/).

[8] "Omada Health chooses Chromebooks to grow its business," March 11, 2014 (https://cloud.googleblog.com/2014/03/omada-health-chooses-chromebooks-to.html); and "The Roche Group goes Google," (https://gsuite.google.com/customers/the-roche-group/).

Outsourcing and Consultants May Not Be the Answer

In the very short term, hiring a security consultant to come in to assess risk and implement mitigations is one option. Organizations such as the HITRUST Alliance may be able to help find such a person. This should not be considered the end of the problem, but rather a starting place. Finding the "right" consultant is not an easy task. There is no reliable set of criteria that would distinguish a consultant who is not only generally qualified, but has sufficient abilities to understand the distinctive aspects of your organization, in order to understand and implement the risk mitigation mechanisms. And further, consultants, by definition, are typically adjunct to the organization, and come in to do something and then leave. In contrast, security must be continuous, ongoing, and deeply ingrained.

In my opinion, the most effective approach for the long term is for organizations to partner together to work on common, secure infrastructure, practices, and procedures that are both broadly effective *and* broadly implementable. A "lowest common denominator" implementation that only reaches the "compliance" bar is no longer a viable option.

Security Is the Responsibility of the Entire Organization

One extremely important point is that security needs to be the responsibility of the entire organization, not just the people who have "security" in their job title. This distinction is not unlike the responsibility of all personnel with regard to patient safety—it is not just the role of the physician and nurse, but includes everyone from purchasing representatives to custodial staff.

Given that computer network-connected devices, from computers running EHRs to network-connected sensor and imaging equipment to HVAC systems, are critical to the function of a hospital for providing high-quality patient care, it is similarly the responsibility of the entire organization to ensure cybersecurity as well.

Conclusions

What should healthcare institutions do? First and foremost, it is vital that executives and boards learn to embrace security rather than resist it. Effective security need not be burdensome,[9] and can even be an *enabling* technology, not unlike how cleaning the oil filter in a car can do double duty for reducing emissions *and* making the car perform more responsively.

Second, find partners so you are not going it alone.

Hospitals need no longer necessarily install and maintain all of their own, internal computer systems—something that has long been both costly and error prone. Google has email, calendars, and collaborative document editing in the cloud. While there are not yet robust, reliable cloud solutions for everything, the list is growing, and most organizations should be asking themselves, for each piece of software, if they should be running that software in-house, and assuming internal responsibility for securing the infrastructure and the data processed by and/or stored on it, or if it might be better run by a major cloud provider such as Amazon, Google, or Microsoft.

And, in many cases hospitals need no longer maintain as many traditional "computer systems" at all. There is almost a complete lack of malware that effects Apple's iOS operating system, for example, and unlike past arguments about the lack of malware affecting MacOS due to low market penetration, the same argument cannot be made about iOS. And the reason is not because of better "security software"—there is effectively none, or at least no anti-virus or traditional monitoring software[10]—but due to the ways in which iOS is more locked down and the iOS App Store has basic curation elements. To be sure, no one would claim

---

[9] Edward B. Talbot, Deborah Frincke, and Matt Bishop, "Demythifying Cybersecurity," *IEEE Security & Privacy*, Vol. 8, No. 3, pp. 56–59, May/June 2010.

[10] Rich Mogull, "Tidal Forces: Endpoints Are Different—More Secure, and Less Open," January 18, 2017 (https://securosis.com/blog/tidal-forces-endpoints-are-different-more-secure-and-less-open).

that iOS is *secure*—no-non-trivial piece of software is. But it does appear to have key advantages. Given all this, what might a world look like in which data is largely stored on large, centrally monitored systems by professionals with experience comparable to those from the best companies and institutions in the U.S., and access to that data were mostly via highly-locked down iOS and other mobile devices?

The Governance Institute thanks Sean Peisert, Ph.D., Staff Scientist at Lawrence Berkeley National Laboratory, for contributing this article. He can be reached at sppeisert@lbl.gov. The full article will be available in December at www.governanceinstitute.com/TGIBoardRoomPress.

■■■

Governance Institute Advisor Spotlight: Guy M. Masters, M.P.A.

In this series, we are spotlighting each of The Governance Institute advisors to give you a look into their roles, expertise, and experience in the industry. The advisors are healthcare experts, each with their own areas of focus, who work with members to help them solve their governance challenges—everything from developing leadership skills to building a competency-based board to assuring best-fit strategic plans and partnerships. Our advisory services include:

- Board education and development retreats
- Independent governance review and redesign processes
- BoardCompass® consultation and self-assessment retreats
- Phone and email consultations
- Specialized consultations

In this article, we highlight Guy M. Masters, M.P.A., Principal at Premier, Inc. Watch for future articles in this series to learn more about each of our advisors.

Industry Expertise

Guy M. Masters, M.P.A., is a Principal in Premier's west coast healthcare management consulting practice. With 30 years of healthcare experience, he focuses on strategic, business, and service line planning; transaction advisory; mergers; board/governance issues; and competitive positioning strategies for hospitals/health systems, physicians, and payers. He has developed HMOs, IPAs, MSOs, PHOs, IDNs, CINs, medical groups, and direct contract relationships with employers.

Guy is an experienced facilitator of board retreats, conducting strategic planning processes, and forming clinically integrated networks. He also executes physician/hospital alignment strategies, implements growth and operational efficiency strategies, and when required, has closed and re-purposed financially troubled hospitals. He is a frequent speaker at industry conferences, professional associations, and other meetings nationwide.

Some of his typical strategic advisory engagements with boards and healthcare executives include:

- Assisting boards in becoming repositioned in the transformation to value based care and payment.
- Strategic and financial planning (setting priorities, facilitating resource allocation decisions, and modeling financial impacts).
- Business plans of operational efficiency—achieving economies of scale, eliminating duplication, and eliminating waste.
- Affiliations without merger (designing multi-hospital/system clinically integrated networks).
- Addressing strategic options for remaining independent.

Work with The Governance Institute

Guy is a regular contributor to *BoardRoom Press* and other Governance Institute newsletters and publications. Most recently

he wrote articles on essential governance considerations for MACRA and the quality payment program, strategic considerations under a new administration's policies, and top trends driving board strategic priorities. In 2016 he co-authored an article on leveraging board effectiveness by increasing committee communication, and wrote an article on MACRA physician payment reform considerations for strategy, financial risk, and physician alignment. Guy contributes his expertise to the Governance Institute's E-Briefings newsletter every January with an article about top healthcare trends for the year. He will also be co-authoring The Governance Institute's Fall 2017 white paper on accountable care organizations.

For almost 20 years, Guy has spoken frequently at Governance Institute conferences. He presented at the 2016 Leadership Conferences on "Board Basics for Effective Governance." These presentations reviewed the framework and context for board responsibilities and accountability around the primary fiduciary responsibilities, defined traditional areas of board best practices, and described the primary drivers of change surrounding healthcare reform and their impacts on board considerations. In addition, Guy spoke at 2016 Leadership Conferences about strategy vs. culture, advanced strategic planning, and creating organizational alignment with physicians in health systems. He also spoke at the 2016 Governance Support Forum on "Creating a World-Class Board: Developing & Implementing an Extraordinary Orientation & Education Plan" where he provided tools, processes, and resources to help governance support professionals improve board education and effectiveness.

In addition, Guy provides on-site governance consulting, governance support to members, and is a board retreat facilitator. This year, he spoke to Governance Institute members at board retreats about high performing boards and board self-assessment and development.

For more information or to schedule an advisory service, contact The Governance Institute at info@governanceinstitute.com or call (877) 712-8778. A detailed list of our advisory services can also be found on our Web site at www.governanceinstitute.com/AdvisoryServices.

■■■

Upcoming Events

Leadership Conference
The Ritz-Carlton, Naples
Naples, Florida
January 14–17, 2018

Leadership Conference
Fort Lauderdale Marriott Harbor Beach Resort & Spa
Fort Lauderdale, Florida
February 18–21, 2018

Leadership Conference
Fairmont Scottsdale Princess
Scottsdale, Arizona
March 11–14, 2018

Click here to view the complete programs and register for these and other conferences.

Upcoming Webinar: The Curious Case of the Healthcare Consumer

December 6, 2017
2:00–3:00 p.m. Eastern Time/11:00 a.m.–12:00 p.m. Pacific Time

The healthcare consumer is often discussed; rarely understood. At a time when consumers are impacting healthcare more than ever, the mentality and motivations of these everyday people are still lost on many organizations. This Webinar will diagnose the healthcare consumer and debunk the most common consumer myths plaguing leaders and board members today. You'll hear surprising trends on consumers' top values and uncover a framework for enabling consumers to make better decisions—including the decision to become a patient.

Register for this Webinar.

■■■

New Publications and Resources

Governance Support: A Behind the Scenes Guide to Ensure Your Board is Prepared, Second Edition (*Elements of Governance*, November 2017)

Board Job Descriptions & Committee Charters, Third Edition (*Elements of Governance*, October 2017)

BoardRoom Press: Volume 28, No. 5 (*BoardRoom Press*, October 2017)

Governance Notes (Governance Support Newsletter, October 2017)

To see more Governance Institute resources and publications, visit our Web site.

■■■