General Counsel Agenda

A Quarterly Legal Perspective on Today’s Top-of-Mind Issues

June 2014

Christine Burke Worthen
Broad and Cassel
cworthen@broadandcassel.com

Mark Hedberg
Hunton & Williams, LLP
mhedberg@hunton.com

Peter Enko
Husch Blackwell
peter.enko@huschblackwell.com

Wakaba Tessier
Husch Blackwell
wakaba.tessier@huschblackwell.com

Sara Shanti
Drinker, Biddle, & Reath, LLP
sara.shanti@dbr.com

Laura Colombell Marshall
Hunton & Williams, LLP
lmarshall@hunton.com

Deborah Juhnke
Husch Blackwell
deborah.juhnke@huschblackwell.com

Julian “Bo” Bobbitt, Jr.
Smith Anderson
bbobbitt@smithlaw.com
Meaningful Use, False Claims, and Cyber Crime – Oh My!
Explore Strategies to Avoid IT Legal Pitfalls

The Health Care Law Roundtable is pleased to present the 2014 second quarter edition of the General Counsel Agenda, a publication written for the hospital and health system in-house counsel audience. The Agenda offers legal analyses on a broad set of pressing issues in health care law, allowing your organization to stay abreast of the top concerns facing providers nationwide.

In this edition, we explore recent regulatory and compliance challenges regarding IT. From the most up-to-date information on potential liability under Meaningful Use to Meaningful Use audit prevention and preparation, experts highlight actionable recommendations for your team. We also spotlight the recent rise in cyber crime and discuss effective strategies to enhance cybersecurity. In addition, our experts discuss legal considerations for nonprofit providers in establishing “reasonable compensation” practices – an issue garnering recent attention from the Office of the Inspector General. Lastly, our experts make the case for hospice and palliative care’s inclusion in ACOs’ strategic endeavors.

Table of Contents

- Attestations and Potential Liability Under Meaningful Use ................................................................. 3
- Meaningful Responses to Meaningful Use Audits .................................................................................. 4
- How Providers Should Respond to Cyber Crime .................................................................................. 5
- “Reasonable Compensation” for Nonprofit Providers ........................................................................... 7
- The Accountable Care Guide for Hospice & Palliative Care ................................................................. 8
Attestations and Potential Liability Under Meaningful Use

Steps to Minimize False Claims Act Liability as a Meaningful User

Laura Colombell Marshall
Hunton & Williams, LLP
lmarshall@hunton.com

Mark Hedberg
Hunton & Williams, LLP
mhedberg@hunton.com

The Attestation Requirement

The Health Information Technology for Economic and Clinical Health (HITECH) Act includes provisions intended to promote the adoption and use of electronic health records (EHR). Using a carrot and stick approach, the Act provides for Medicare incentive payments to promote the “meaningful use” (MU) of certified EHR technology, as well as penalties that will impose Medicare reimbursement reductions on “eligible professionals” (e.g., doctors) (EPs) and hospitals (EHs) who are not meaningful users of certified EHR technology beginning October 1, 2014 for EHs and January 1, 2015 for EPs. EHs and EPs must continue to demonstrate meaningful use every year to avoid payment adjustments in subsequent years.

MU is demonstrated through a web-based system whereby data is entered regarding applicable objectives and measures and the EP or EH “attests” that they have used certified EHR technology (including specification of the technology used) and satisfied the required objectives and associated measures, as well as agreeing to the following attestation statements (among others):

- The information submitted is accurate to the knowledge and belief of the EP or the person submitting on behalf of the EP or EH;
- The information submitted is accurate and complete for numerators, denominators, exclusions, and measures applicable to the EP or EH; and
- The information submitted includes information on all patients to whom the measure applies.

False Claims Act Liability

The February 2014 indictment of a CFO for a now closed medical center in Texas for making false statements and committing aggravated identity theft in connection with Medicare MU payments increased speculation that CMS meaningful use compliance audits would result in referrals to law enforcement for investigations under the False Claims Act (FCA). The indictment alleges that the CFO forged the signature of the center’s Director of Nursing on the MU attestation after she refused to sign because she knew the center’s EHR technology was not compliant. While the case appears to be a factual outlier, it does signal that the government is receptive to prosecuting cases stemming from false MU attestations.

In addition to the attestation statements listed above, an EH or EP must also acknowledge that the filing of the attestation itself equates to submitting a claim for federal funds, and that any false statement in the attestation is punishable under federal or state criminal laws and subject to civil penalties. A false MU attestation is therefore clearly material to the claim as a precondition of the EHR incentive payment. Liability can also arise from a “reverse false claim” which now includes the knowing retention of an overpayment. In order to properly assess the risk of an FCA investigation or action, it is important to understand the requisite intent under the statute. The terms “knowing” and “knowingly” are specifically defined in the statute to include “deliberate ignorance” or “reckless disregard” of the truth or falsity of the information. As a practical matter, this means that it is not enough for the attester to wholly rely on the representations of a vendor or employee to certify that a provider has met the MU requirements under the EHR program.

Although not an FCA case, the 2013 repayment of millions in MU payments by a large for-profit provider demonstrates the severe financial risk associated with noncompliance. The for-profit provider’s repayment was the result of an internal audit which revealed that the company received MU payments for multiple hospitals over a three-year period which had not met the applicable criteria. The provider cited a “material weakness in internal control related to the administration and oversight of its EHR enrollment process” and stated that an error was made in applying the MU requirements. The exact nature of the compliance lapse is unclear. However, the EHR program requires full recoupment of incentive payments in the event of partial noncompliance.

Medicare and Medicaid audits of MU payments began in 2013 and will continue. EHs and EPs will be selected at random for audit and required to produce documentation to support the attestation. An FCA investigation can result from these audits or from a whistleblower looking for a qui tam opportunity. Prosecutors will be looking for aggravating facts that will escalate a compliance issue into a full blown criminal or civil enforcement action. In this regard, EHs and EPs should be looking for any conduct that arguably creates the false appearance of EHR
compliance, such as entry of data from hard copy records “after the fact” or copying and pasting data from one patient visit to the next.

In light of the potential for significant liability in this area, EPs and EHs should, at a minimum:

• Implement internal processes to capture, verify and document the data that supports a MU attestation, with careful consideration of the supporting documentation for audits guidelines provided by CMS.

• If a provider identifies a compliance issue after the attestation has been made, determine whether it is the result of a benign error or some systemic failure that could be interpreted as fraudulent. This determination is critical in determining next steps and how best to mitigate liability under the FCA for damages and penalties.

• Conduct compliance due diligence with respect to MU payments received by a target company in a proposed acquisition or joint venture. Given the potential risk, such an audit could inform whether the deal should go forward, or at the very least factor into the valuation.

Meaningful Responses to Meaningful Use Audits

How Providers Can Address Meaningful Use Audits and CEHRT Security

Sara Shanti
Drinker, Biddle, & Reath, LLP
sara.shanti@dbr.com

The U.S. Department of Health and Human Services (HHS) has renewed its commitment to review meaningful use incentive payments in 2014. Last year, the Centers for Medicare and Medicaid Services (CMS) announced that HHS would conduct prepayment audits of 5-10 percent of those who attested to meaningful use under the EHR Incentive Program (Program) and post payment audits of another 5-10 percent of attesting participants. HHS’s Office of Inspector General (OIG) subsequently announced its intention to audit the security of certified EHR technology (CEHRT) of recipients of Program incentive payments. Focus on CEHRT security has been seen first-hand in HHS’s increased meaningful use audit activity, with a specific emphasis on the protection of electronic protected health information (ePHI) maintained within Program participants’ EHRs. These audits risk Program incentive payment denial as well as the recouping of previous incentives – amounts which may significantly impact providers’ anticipated EHR objectives or financials. OIG’s concentration on the adequate protection of ePHI created and maintained by CEHRT is likely the result of a chief concern identified in the first round of the CMS audits, as well as the recent implementation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Final Rule, numerous high profile security breaches, and the growing popularity of cloud-based EHR technologies and vendors. Effectively, while the heart of the CMS audit remains the Document Request list requiring documentation supporting the completion of many or all of the Program’s Core Set Objectives and provider attestations, CMS and OIG are now particularly interested in Core #15 – Protect ePHI. This Core Measure specifically requires the production of evidence that a HIPAA Security Rule risk analysis has been performed for the reporting period. Additionally, providers must be prepared to submit evidence of the implementation of security plan and/or updates necessary to correct security deficiencies identified in the risk analysis. To date, HHS has provided little guidance as to what constitutes a compliant HIPAA risk analysis and has maintained HIPAA’s flexible approach.

The flexible approach allows entities wide breadth in how the risk analysis is performed; however, “generalized” information will not meet the requirement. At minimum, providers must (i) identify the system(s) that access, transmit, and maintain ePHI; (ii) identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI; and (iii) implement reasonable and appropriate mitigation steps to reduce identified risk. The risk analysis must address internal and external threats to ePHI, such as environmental, human, and technological, as well as the existence or lack of encryption taking into consideration the practice’s size, complexity, and capabilities. Risk analyses must also be revisited and updated on a reasonable basis and upon any change to the provider’s system(s).

Notwithstanding the preceding elements, the risk analysis does not need to adhere to a precise form or be contained in a single document, and the methodologies and processes used to perform the analysis may vary. Clear documentation is, however, paramount. Because compliance with this measure requires the risk analysis be performed prior to the end of the reporting period, entities should take care to ensure the documentation is dated and distinguished from one reporting year to another. Although the audits may request documentation within a short timeframe (approximately 30 days for the initial response, and as short as a few days for supplemental requests), entities can take simple preparatory measures to ensure an audit response meets the requirements.
Steps to Prepare for an Audit and Provide a Meaningful Response on CEHRT Security

- Conduct and/or update the HIPAA risk analysis for each Program participation year.
- Ensure the risk analysis is dated and specific to the certified EHR and Program participant. HHS has stated that “[i]nformation that is dated and specific to [the practice] goes a long way for a lot of these requirements.”
- Document security implementation plan(s), including proposed dates of completion.
- Identify and update other supporting documents addressing CEHRT security such as:
  - Privacy and security policies and procedures;
  - Safeguard mechanisms;
  - Back-up, emergency, and recovery plans;
  - EHR vendor agreements and business associate agreements; and
  - Mitigating and corrective action measures.
- Obtain copies of EHR certification and vendor licensing agreements and invoices.
- Identify related areas of potential CEHRT regulatory noncompliance (e.g. fraud and abuse, HIPAA).
- Retain screenshots demonstrating enabled capabilities, including capture of EHR monitoring capabilities.

Audits continue to be conducted at random and in response to suspicious or anomalous attestation data. Because they are also conducted on both postpayment and/or prepayment bases, in some cases, an entity will receive a prepayment audit on the heels of completing its response to a postpayment audit, or vice versa. Therefore, it is extremely important to ensure the documentation submitted for the applicable reporting year addresses the CEHRT security related to that specific year. A red flag, easily identified by the auditors include identical risk analyses for two or more years. Although HIPAA does not expressly require a risk analysis be performed annually, meaningful use requires annual attestation of such. Effectively, at minimum, it should be noted that the risk analysis was reviewed on an annual basis to determine whether revisions are necessary.

In conclusion, attesting Program participants are encouraged, more than ever, to review HIPAA risk analyses for completeness and update the information in a timely manner, addressing the security matters for each reporting year, to ensure full Program payments and avoid regulatory liability.

How Providers Should Respond to Cyber Crime

Ways to Mitigate the Negative Consequences of Hacking, Data Breaches, and Theft

Deborah Juhnke
Husch Blackwell
deborah.juhnke@huschblackwell.com

Wakaka Tessier
Husch Blackwell
wakaka.tessier@huschblackwell.com

Peter Enko
Husch Blackwell
peter.enko@huschblackwell.com

Hacking. Breaches. Theft. Cyber crime is more prevalent and visible than ever before. The response to these threats, as noted in the 2014 Mandiant Threat Report, is that “[c]yber security has gone mainstream.” And while no security effort is perfect, there are ways to help identify and mitigate risks.

The Kill Chain Framework

“A kill chain is a systematic process to target and engage an adversary to create desired effects.” The kill chain concept, developed in a Lockheed Martin white paper and referenced by the Senate Committee on Commerce, Science, and Transportation in its analysis of the 2013 Target Data Breach (“Target Report”), offers a systematic approach to identifying and mitigating cyber security risks.

In November and December of 2013, hackers executed a successful attack on Target, stealing data on 40 million credit and debit cards and also sensitive information of 70 million customers. The Target Report applied Lockheed Martin’s “kill chain” framework to known events and determined at which points Target apparently failed to detect and stop the attack. This retroactive analysis revealed that, while Target likely failed at multiple steps along the chain to stop the breach, the opening salvo by the attackers was waged not on Target but a Target vendor, Fazio Mechanical Services.
The Target Report suggests that the attackers may “have sent malware-laden emails to Fazio at least two months before the Target data breach began.” Target’s supplier portal and facilities management pages were apparently viewable on the Internet and available metadata “allowed the attacker to map Target’s internal network prior to the breach.” Unfortunately, Fazio was also using a free anti-malware product, which did not provide real-time protection and was intended only for individual consumer use.

A “Heartbleed” Away From Data Disaster

Organizations may also look to the kill chain framework as a resource in addressing the recent “Heartbleed” vulnerability. The Heartbleed bug has gained substantial media coverage, and organizations, especially those in healthcare, should pay special attention to its risks. Notably, Heartbleed is a software defect and not a hack attack. This flaw in the OpenSSL library - used by security vendor products to secure web browsing and mobile banking applications - went unnoticed for years, during which time the software was adopted by about a half million websites. Thus, the kill chain for Heartbleed started long ago when the deficient software was first introduced into trusted domains.

Though not an attack per se, Heartbleed did open a door to hackers and there has been at least one publicized effort in Canada to use the vulnerability to steal tax IDs - by a 19-year-old teenager. When the Heartbleed bug is exploited, the attacker may retrieve up to 64KB of memory from the remote system. Such information may contain usernames, passwords, and keys that enable even larger attacks.

Heartbleed Mitigation and Response

Although the technical response to the Heartbleed bug is beyond the scope of this article and should involve internal and external information technology and security experts, effective risk mitigation strategies involve more than technical patches. Organizations subject to regulatory and industry oversight should first confirm their obligations regarding notices to affected individuals about the need to change passwords to prevent future exposure. Moreover, if the Heartbleed defect was in fact exploited in a manner that disclosed protected information, breach notification requirements, such as those set forth in HIPAA, must be considered. Finally, with the FTC’s increased interest in monitoring corporate privacy and security practices, even non-regulated organizations should take steps to ensure that their websites and portals do not subject customers to potential breaches.

If a security risk assessment reveals an organization’s system was not affected by the Heartbleed bug, the organization still should consider taking steps to address the potential security risk. For example, employee credentials used to log into a third party system with Heartbleed might have been compromised and might expose an organization’s sensitive information and IT system to risk.

Vigilance is Vital

Recently, additional vulnerabilities have surfaced related to OpenSSL that allow an attacker to create a denial of service condition, making a server unavailable to its intended users. These new defects may also facilitate remote code execution, which enable an attacker to run unauthorized programs on an organization’s computer.

The implicit message of the Target breach, Heartbleed, and countless other reported and unreported security incidents is that no system is completely secure. The Target Report clearly demonstrated that the weakest link may be outside of the organization, and that the key to avoiding a security breach is to detect and address any problems before they occur. Because prevention is predicated on knowledge, the kill chain framework used by the Senate committee to analyze the Target breach retroactively may also prove a useful tool in identifying vulnerabilities before a breach happens. In particular, four data privacy and security risk management recommendations flow from the kill chain analysis:

1. Planning and Preparation — Do a risk assessment to identify and minimize the amount of unprotected information available through the Internet. Ensure that your organization has a comprehensive information security plan and review contracts to be certain that security and breach response are addressed. Review insurance coverages.

2. Technology Controls — Adhere to all applicable IT standards and keep all systems patched. Invest in appropriate tools (usually not free!) and know where your organization’s data is located.

3. Vendor Management — Limit and control vendor access to your organization’s IT system by, among other things, eliminating single log-on ids.

4. Training and Awareness — Most vulnerabilities involve a human element and training is an essential first line of defense. Preach “phishing” awareness and secure password use and be sure to audit and enforce policies. Remember, the Target breach likely began with a single user opening a single e-mail.
Executive compensation at nonprofit organizations is a topic that garners much attention from time to time. For nonprofit providers, executive compensation arrangements have increasingly come under increased scrutiny since the IRS required annual IRS Form 990s to be publicly available on the organization’s website. Further, some states have undertaken their own reviews of executive compensation of nonprofits in an effort to identify trends and potential issues. With the OIG’s release of its 2014 work plan, which includes a provision to review how executive pay falls within a provider’s operating costs, nonprofit providers may find their executive compensation packages on the OIG’s radar, especially with the potential imposition of caps on the amount of executive compensation that can be included in the provider’s cost report. While caps haven’t been applied in the past, there’s still an existing requirement that in order to be included in the cost report, executive compensation must be reasonable. Given the OIG’s work plan, now is a good time to review executive compensation packages and processes to ensure that compensation paid is reasonable.

With regard to the OIG work plan and executive compensation in particular, the OIG indicated that it will be analyzing the potential impact on the Medicare Trust Fund if the amount of employee compensation that could be submitted to Medicare for reimbursement on future cost reports had limits. While the OIG indicates that the context of its review is to ensure that employee compensation is included in allowable provider costs only to the extent that it represents reasonable remuneration for managerial, administrative, professional, and other services related to the operation of the facility and furnished in connection with patient care, there is industry buzz that the work plan is the result of letters sent to several nonprofits hospitals in 2013 asking them for information on their highest paid executives dating back to 2008. While it is premature to draw conclusions as to the results that the OIG will publish in 2015, the inclusion of executive compensation as an item on the 2014 OIG work plan serves as a good reminder that nonprofit providers must exercise due diligence in setting executive compensation packages not only for the sake of public scrutiny, but also to avoid penalties and possible revocation of tax exempt status under federal income tax laws and regulations.

As part of the process of designing and implementing executive compensation packages for nonprofit hospital and healthcare system executives, consideration must be given as to whether and to what extent the package could result in prohibited private inurement or expose the arrangement to intermediate sanctions under the Internal Revenue Code of 1986, as amended, and the Treasury Regulations promulgated thereunder. An organization faces loss of tax-exempt status if it engages in prohibited private inurement, which means that the earnings of the tax-exempt hospital inure to the benefit of private individuals. Tax-exempt providers may pay reasonable compensation for items and services. If they pay more than reasonable compensation, the excess amount may be prohibited private inurement. The existence of private inurement involves a facts and circumstances test, and only applies to private individuals (i.e., “insiders”). Whether an individual is an insider involves an analysis as to whether he/she is an officer or director, or otherwise is in a position to exercise significant influence on the organization’s decision-making process, which would almost always mean that “healthcare executive” meets this definition. Private inurement can jeopardize the tax-exempt status of the entity. Intermediate sanctions involve a tax penalty and correction of the excess benefit. If a disqualified person (one who is in a position to exercise substantial influence over the organization) receives a benefit that is in excess of the benefit received by the provider, then there would likely be an excess benefit. An evaluation of the facts and circumstances to determine whether or not the executive meets the definition of a disqualified person (similar to the exercise under the evaluation of private inurement) would be the first step. If the executive meet the definition of a disqualified person, then the next step would be to determine if there is an excess benefit transaction. If there is an excess benefit transaction, then the organization will want to examine whether it can meet the rebuttable presumption test which would indicate that the compensation was reasonable (i.e., the compensation was approved in advance by an authorized body that relied on appropriate data for comparability, and the entire process was adequately documented). If there’s an excess benefit transaction, the taxes can be steep – from 25-200+ percent of the amount of the excess benefit. There are correction methods which might be available to mitigate the tax and limit to the penalty as long as the insider returns the excess benefit to the provider within the...
The review and scrutiny of executive compensation at nonprofit hospitals and healthcare systems has been done primarily by the IRS. However, with the addition of executive compensation as a new item on the OIG 2014 work plan, and uncertainty as to what this might mean, nonprofit providers should ensure that a process is in place, preferably through a compensation committee, to conduct an analysis of any proposed compensation arrangement with their executives. Taking steps to ensure that an executive compensation package is reasonable can serve to ensure that an organization would be less likely to have issues from a revocation of tax exempt status perspective as well as an excise tax perspective. In the event the review outlined in the OIG 2014 work plan results in the implementation of parameters for executive compensation for cost reporting purposes, nonprofit providers who have taken steps to ensure that reasonable compensation will likely be in a good position. While it’s premature at this stage to make material changes to existing executive compensation packages based on the inclusion of executive compensation in the 2014 OIG work plan, nonprofit providers should undertake processes to ensure that executive compensation is reasonable not only to ensure compliance with existing federal tax laws and regulations, but also to ensure that the right compensation packages offered take into account the myriad of changes that our healthcare delivery system is undergoing and the payment structure for executives who will be a part of it.

The Accountable Care Guide for Hospice and Palliative Care

Ways ACOs Can Include Hospice and Palliative Care in Strategic Endeavors

Julian “Bo” Bobbitt, Jr.
Smith Anderson
bbobbitt@smithlaw.com

Our nation’s in the midst of an inexorable shift in health care delivery from fee-for-service (FFS) to “fee-for-value.” Our current FFS system is unsustainable and an incentive shift must occur to encourage providers to be committed to providing the highest quality at the lowest overall cost through seamless integration across the continuum of care. An emerging model to achieve these goals is the accountable care organization (ACO), which consists of providers jointly accountable for achieving measured quality improvements and reductions in the rate of spending growth. This article explores the significant opportunity in including hospice and palliative care in ACO endeavors.

The Case for Hospice and Palliative Care in ACOs

ACOs are beginning to focus on post-acute care generally, and hospice and palliative care in particular. The following information helps make the case for greater emphasis on hospice and palliative care in value-based care:

- $50 billion, ~10% of Medicare funds, is the annual spending on the last month of patients’ lives;
- 65% of health care spending goes toward the sickest 10% of patients, an average of $157,510 annually per patient;
- 65% of poor-prognosis cancer patients are hospitalized during the last month of life;
- 25% of poor-prognosis cancer patients use a hospital intensive care unit during the last month of life;
- 30% of poor-prognosis cancer patients die in the hospital; and
- $5,000-7,000 is the annual savings per patient when palliative care is provided alongside usual care.

The Role of Hospice and Palliative Care in an ACO

In the value-based reimbursement era, stakeholders are rethinking their roles. The top five high-yield targets for ACOs include:
• Wellness/prevention,
• Chronic care management,
• Reduced hospitalizations,
• Care transitions, and
• Multi-specialty coordination of complex patients.

Providers should prioritize targets based on success elsewhere (e.g., the quickest and biggest results, proven metrics, and community health care leaders willing to champion the effort). This should reveal a potential prioritized list of value-add ACO initiatives. The last step is to marry them in a particular locale through a gap analysis to the areas of avoidable waste in that region.

The Top Value-Add ACO Initiatives for Hospice and Palliative Care

The top value-add ACO initiatives involving hospice and palliative care include:

1. Using Interdisciplinary Teamwork as a Model – Hospice and palliative care are well-prepared for integration into ACOs. Hallmarks of good palliative care include teamwork and the ability to form partnerships across the care continuum. Hospice and palliative care can operate as a model of interdisciplinary teamwork that could serve as an example for other providers in their specialty areas.

2. Adopting Chronic Disease Management Best Practices – Palliative care excels in chronic disease management and end-of-life care. Many hospice and palliative care patients have complex illnesses requiring coordinated, interdisciplinary management. Palliative care programs positioned across the care continuum have been valued, successful components of bending the cost curve. Care discussions often lead patients to choose less invasive/aggressive care paths, thereby avoiding unnecessary procedures and hospitalizations while aligning therapies concordantly with care goals. Effective symptom management, regardless of the setting, provides patients and families critical support and decreases excessive expenditures. Also, palliative care decreases readmissions and length of stay, while increasing quality of life and life span. Ultimately, the use of palliative care decreases the use of high-cost, low value treatments resulting in enhanced efficiency.

3. Educating and Engaging Patients and Family – An emphasis of ACOs is patient-centered care aimed at creating partnerships between patients and physicians. Palliative care focuses on determining patients’ needs to help formulate care plans.

Palliative care also emphasizes patient and family education as a means of achieving the patient-centered goals of care and preventing unnecessary care. Palliative care affords an opportunity for patients and families to be introduced to advance care planning questions including designation of surrogate decisions makers and completion of MOST/POLST type documents. Pain and symptom management and patient and family education training are both linked to increased patient satisfaction and cost reduction at the end of life. Patient adherence to a care plan and self-management helps drive down healthcare costs.

4. Engaging Providers – ACOs rely on active involvement and communication of all providers involved in a patient’s care plan since many different stakeholders are responsible for shaping each patient’s care experience. Palliative care providers are accustomed to this collaborative model because palliative care is built on the ability to analyze a situation from multiple stakeholder perspectives and respond appropriately. This model helps overcome territorial barriers specialist providers may feel concerning their patients. Also, through education, providers can learn about the wealth of palliative care resources available to their patients concurrently with curative treatment.

5. Avoiding Expensive Drugs and Procedures with Marginal Value – Opportunities for improved care and cost also exist in pharmacy and procedure selection. Polypharmacy and use of unnecessary procedures often adds to patient suffering. Palliative care focuses on improving quality of life through reduced symptom burden and supportive care. This value-based thinking will benefit the patients clinically and financially and benefit the shared savings.

6. Leveraging Experience with Data Management – ACOs can leverage technology with accurate, reliable data. To make care improvements and establish appropriate metrics, ACOs must carefully track and analyze patient population data. Palliative care has developed effective tools for collecting data based on its need to demonstrate cost savings and effectiveness and, thus, justify its value.

Hospice and Palliative Care Performance Metrics

• Avoidance of admissions for CHF and COPD
• Critical care usage and costs
• Pose accurate episodes of care cost reductions
• Laboratory costs
• Imaging costs
• Pharmaceutical costs
• Chemotherapy in the last month of life
• Use of percutaneous feeding tubes in advanced dementia
• Use of MOST/POLST in the last year of life
• Following use –of-hospice guidelines for the last six months of life
• Percentage constipated on pain meds
• Survey – meeting the needs of patients and families results
• Length of stay over 14 days
• Hospital readmission reduction
• Electronic information exchange

**Conclusion**

For good reason, post-acute care generally, and hospice and palliative care particularly, are becoming regarded as important contributors to ACO success in raising quality and bending the health care cost curve. Hopefully, this short article has helped illustrate the significant upside potential for involving hospice and palliative care in ACOs.