E-Briefings

Volume 11, No. 5, September 2014

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. Please note that you are receiving this newsletter because you are a Governance Institute member or expressed interest at one of our conferences.

In this issue:

Disruptive Innovation in Healthcare: Are You Ready?

By Jon Burroughs, M.D., M.B.A., FACHE, FACPE, The Burroughs Healthcare Consulting Network, Inc.

Clayton M. Christensen, Professor of Business Administration at the Harvard Business School popularized the term "disruptive innovation" to mean options that are: lower cost, more convenient and accessible, and of "good enough" quality to satisfy a customer. You may ask, "But don't we want everyone to receive the best that healthcare can offer? Why would anyone want second best?"

The answer lies in the Institute of Medicine's definition of quality in *Crossing the Quality Chasm* that it should be: safe, timely, effective, efficient, equitable, and patient centered. Still today, this is something few organizations offer and even fewer individuals can afford. Thus, the market seeks new options that significantly lower the cost; improve accessibility, efficiency, and service; and don't excessively sacrifice quality. Enter disruptive innovations, which become the new "good enough" options and become the new "normal."

The following are brief examples of how the current business models in healthcare are already being disrupted and why these changes will be significant and swift.

1. The Hospital

The hospital emerged as a fundamental healthcare business model in the early 20th century when scientific progress permitted the effective diagnosis and treatment of common diseases and surgical conditions. Thus, a hospital bed was surrounded by a clinical laboratory, ancillary services, specialty consultants, and operating suites to create a one-stop diagnostic and therapeutic venue within which physicians could ply their craft as individual "experts." The challenges with this traditional model are that care is expensive (high in fixed costs), inefficient (lack of coordination and integration), of mixed quality/safety/service (based upon variation among practitioners and inherent complexity), and slow to respond to market demand (due to cumbersome bureaucracy). As a result, the following innovations are taking place throughout the country:

- Emergence of ambulatory facilities to provide routine high-volume, low-risk procedures for defined entities (routine surgeries, catheterizations, urgent care) at a lower cost, greater efficiency, and more reliable outcomes
- Growth of specialty hospitals and integrated healthcare systems (e.g., Cancer Centers of America, Mayo Clinic) to provide high-quality/low-cost integrated and coordinated healthcare for commonly encountered conditions
- Growth of palliative and hospice care units to provide low-cost and compassionate care to those with terminal conditions
- Growth of retail clinics (e.g., MinuteClinics) to offer individuals 24/7 access to urgent care for commonly acquired conditions

- Growth of domestic and international medical tourism to divert patients to lower-cost/high-quality venues throughout the country and abroad as an alternative and based on significant cost savings incentives for employees and beneficiaries
- Growth of disease management and population health programs with incentives to significantly reduce inpatient and ED volumes

2. The Physician's Office

The heart and soul of 20th century healthcare was the physician's office and the relationship between the patient and his/her physician. Even the hospital was considered the physician's "workshop" and an adjunct to this core service interaction. This fundamental relationship is being questioned due to: variation among the quality, care, and service that different physicians provide, the increasing cost of maintaining this relationship (e.g., concierge practices), the potential inconvenience (third available appointment rates), the lack of access (shortage of physicians in many areas), and the lack of patient-centered approaches due to the traditional mantra that the "doctor knows best." As a result, the following innovations are taking place:

- Approximately 80 percent of what physicians do can be done by healthcare practitioners with less training and cost (e.g., advanced practice nurses and physician assistants). These individuals typically spend more time with patients, follow evidence-based algorithms, and provide an excellent quality of service.
- Acute and critical care services are now provided by full-time employed physicians in the inpatient setting.
- Approximately 80 percent of what non-physicians do can be performed virtually through cloud-based services. For instance, several organizations implement transactional healthcare services on the Internet or through Web-based applications that enable an individual to be evaluated by a physician or advanced practice nurse through a Webcam, be diagnosed for routine conditions, and be treated, all in the comfort of one's home.
- Ambulatory facilities (walk-in centers and retail clinics) can handle many of the routine clinical conditions that were traditionally handled in a physician's office at lower cost and greater convenience (24/7).
- Domestic and international medical tourism diverts traditionally loyal patients to lower-cost/higher-quality venues through significant financial incentives by large employers and insurance carriers.
- Patient-centered medical homes, accountable care organizations, and acute care episode projects divert patients to lower-cost/higher-quality venues.
- Wireless telehealth technology and implantable monitoring devices permit patients to be monitored and treated at home through centralized home health networks staffed by advanced practice nurses.
- Population health and disease management care requires a complex infrastructure that is beyond what most small physician groups can afford.

3. Fee-for-Service Reimbursement

Many acknowledge that the root cause of our healthcare system being so expensive and our quality outcomes so lackluster is the traditional discounted fee-for-service payment methodology, which rewards physicians and hospitals that provide high-margin care (elective surgeries and ancillary services) at the cost of potentially beneficial preventive healthcare services. Most agree that we will evolve to some form of capitation with incentives. The difficulty is the transition in a world that still rewards those who persist in providing non-evidence-based care that is profitable even if it does not necessarily benefit individuals. Thus, the following payment innovations are occurring:

- Integrated healthcare networks that can offer higher-quality/lower-cost services and sign capitated and bundled agreements with large employers and healthcare carriers (through public and private exchanges), which diverts business away from traditional fee-for-service enterprises and creates new domestic and international medical tourism markets.
- Healthcare systems merge or partner with healthcare carriers to significantly reduce their cost structure and provide lower-cost care by managing their own actuarial risk.
- Healthcare systems consolidate to lower cost and optimize access to high-quality networks.
- Cloud-based services permit access to patients and beneficiaries far outside of traditional service areas at lower cost and greater accessibility.
- Healthcare organizations voluntarily exit fee-for-service to embark upon risk contracts with large employers, healthcare carriers, and CMS.

Conclusion

Disruptive innovation cannot be stopped nor stemmed because it offers services to those who could neither access nor afford healthcare services in the past. Even physicians and healthcare executives acknowledge that the system no longer works and needs to be redesigned. The question is, will there be a coordinated effort to build a rational, value-based network (commercial ecosystem) that works, or will it happen by chance and become a heterogeneous collection of competing entities with a lack of seamless integration and harmony among the component parts? The only way to achieve the former will be for healthcare leaders to embrace disruptive change and to utilize their traditional clinical, operational, and financial skills to build a new healthcare system based upon a unified vision that works, rather than an accidental system built by default.

The Governance Institute thanks Jon Burroughs, M.D., M.B.A., FACHE, FACPE, president and CEO of The Burroughs Healthcare Consulting Network, Inc., for contributing this article. He can be reached at jburroughs@burroughshealthcare.com.

■■■

Terms of Engagement: The Board's Responsibility for Cybersecurity

This is the fourth article in a series examining governance tasks that may now require a heightened level of attentiveness.

By Michael W. Peregrine and Edward G. Zacharias, McDermott Will & Emery, LLP

Cybersecurity issues may have long been a "back-burner" issue for many healthcare boards, but that needs to change—and fast.

An extraordinary series of developments this year is pushing healthcare boards to become much more focused in their attention to, and oversight of, cybersecurity and data protection matters. We are talking about FBI alerts; data breaches at major healthcare systems; numerous reported vulnerabilities of network-connected medical devices; new governance best practices; bar association resolutions; and regulatory enforcement actions, cyber risk-related criticisms of board oversight by senior government officials, and private party litigation. And all that is on top of the steady drumbeat of media stories about major U.S. companies outside of healthcare being "hacked," with the attendant legal exposure to customers (and shareholders).

There simply is no longer any question that cybersecurity must become a "front-burner" oversight concern for the healthcare board. Too much is happening, too fast, and with too much risk at stake for the healthcare system and its constituents—and the security of its healthcare data. We are not talking about something "drummed up" by consultants to generate work. And it is also really not just about adopting internal breach remediation and other mitigation tactics, which are reactionary by nature. What we are talking about is a complete evolution of governance standards as they relate to computer security and its application to protecting patient health data and medical devices. The organizational focus is noticeably moving "from the IT department to the boardroom"—and at a rate of speed that will catch the inattentive board off guard.[1]

The new developments sparking this governance evolution are happening across the commercial sector (including, but not limited to, healthcare), as is demonstrated by the following examples.

Best Practices

Hospital and health system boards are, by their nature, very attentive to new governance

[1] Brad Walz, "Cybersecurity: Having a Privacy Policy Is Not Enough," JD Supra Business Advisor, July 2, 2014; see also Danny Yadron, "Corporate Boards Race to Shore Up Cybersecurity," *The Wall Street Journal*, June 29, 2014.

standards and "best practice" developments. For that reason, new guidelines proposed by the respected National Association of Corporate Directors (NACD) should be brought to the board's attention. In *Cyber-Risk Oversight*, the latest edition of its Director's Handbook Series, NACD strongly endorses a clear board cybersecurity oversight role. This important new publication offers five key oversight principles for corporate board consideration:

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber risk management should be given regular and adequate time on the board meeting agenda.
4. Directors should set the expectation that management will establish an enterprise-wide cyber risk management framework with adequate staffing and budget.
5. Board–management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.[2]

What the Regulators Are Saying

When an SEC Commissioner speaks on the topic of corporate governance, hospital and health system boards should listen—even if they are not directly subject to the SEC's jurisdiction. This is particularly the case with respect to a recent speech by SEC Commissioner Luis Aguilar, encouraging boards to include cyber preparedness as an important element of their risk oversight duties.[3] Noting the many known risks to corporations arising from cyber-threats, Commissioner Aguilar expressed concern that a gap may exist between the magnitude of these risks and the level of board preparedness. In his view, boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility do so at their own peril.

[2] National Association of Corporate Directors, Director's Handbook Series, *Cyber-Risk Oversight*, 2014, p.4.
[3] Luis A. Aguilar, "Boards of Directors, Corporate Governance, and Cyber-Risks: Sharpening the Focus," Cyber Risks and the Boardroom Conference, June 10, 2014.

The FBI's Warning

Of particular importance to healthcare boards is the recent series of warnings from the FBI concerning the exposure of healthcare companies to cyber-attack. The most recent of these warnings was released in late August, on the heels of the public announcement of the attack on patient data of a large national proprietary health system. "The FBI has observed malicious actors targeting healthcare-related systems, perhaps for the purpose of obtaining protected healthcare information (PHI) and/or personally identifiable information (PI)."[4] These FBI alerts serve as increased evidence of the enterprise risks associated with cybersecurity, and must be brought to the attention of the board—even if they were originally addressed to chief information officer and similar corporate officers.

Other Healthcare Developments

Also relevant, from a healthcare governance perspective, is the series of compelling recent computer security risk developments affecting the healthcare sector. Recently, a number of healthcare organizations have been targeted by malicious hackers and subjected to increased scrutiny by regulatory authorities.

As noted above, data on 4.5 million patients was recently stolen when Chinese hackers targeted a major healthcare system's network. While the stolen data did not include medical information, it did include names, addresses, birthdates, telephone numbers, and social security numbers—information that can be used for identity theft and financial fraud. Healthcare organizations have become attractive targets for hackers because they often store as much, if not more, personal information about individuals than traditional targets such as banks, but frequently have less computer security expertise and weaker computer security infrastructures that are easier for hackers to compromise.[5] Lax security systems and practices also make it more difficult to detect and remediate a cyber-attack, giving hackers more time to probe and pull data.

From a liability perspective, regulators and plaintiffs have been active in pursuing claims

[4] Jim Finkle, "FBI Warns Healthcare Firms They Are Targeted by Hackers," *Reuters*, August 20, 2014.
[5] Beth Kutscher and Joseph Conn, "Chinese Hackers Hit Community Health Systems; Others Vulnerable," *Modern Healthcare,* August 18, 2014.

against healthcare organizations that have failed to appropriately secure consumer information. Health plans, most healthcare providers, and healthcare clearinghouses (covered entities) are subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as are their vendors that receive individually identifiable health information in providing services to the covered entity. HIPAA mandates compliance with a set of information privacy and security standards. The Department of Health and Human Services, Office for Civil Rights (OCR) is the primary federal agency responsible for enforcing HIPAA and has been vocal about enforcement being an agency priority.[6] In a press release announcing a 2013 breach settlement with Shasta Regional Medical Center in California, former OCR Director Leon Rodriguez stated: "[s]enior leadership helps define the culture of an organization *and is responsible for* knowing and complying with the HIPAA privacy and security requirements to ensure patients' rights are fully protected."[7]

Healthcare companies have also found themselves "in the crosshairs" of state attorneys general, who now have authority to enforce HIPAA[8] in addition to their traditional jurisdiction over state consumer protection laws and regulations. While most state attorneys general have been slow to embrace their relatively new HIPAA enforcement authority, these actions will likely increase as state regulators become more comfortable with HIPAA. Moreover, a number of state attorneys general are actively enforcing their state's data breach notification laws against healthcare companies.[9] In a recent, notable case, a state whose residents were affected by a breach at a hospital located in a neighboring state sought to enforce its data breach law against that hospital. Last month, the hospital agreed to pay $150,000 to settle the allegations.[10]

In addition to enforcement actions by regulators, a number of lawsuits have also been filed by individual consumers or classes of consumers in response to security breaches. Judges are increasingly throwing these cases out of court in circumstances where the plaintiff is unable to provide evidence that the security event resulted in actual harm.[11] Nevertheless, the litigation surrounding these cases can be time-consuming and expensive. For example, Stanford Hospital and two of its business associates recently agreed to pay $4.1 million to settle a class-action lawsuit arising from a breach that resulted in the medical information of approximately 20,000 emergency room patients being made publicly available on the Internet for a period of nearly a year.[12]

Board Action

The message from these developments is that the healthcare board must "get serious" about providing oversight of the system's cybersecurity measures. There is simply no flexibility here in terms of placing this issue high on the board's agenda item, and soon—there has just been way too much activity for a board to postpone a close focus anymore. The good news is that there is a fairly clear pathway for healthcare boards to follow in response to this evolution. The elements to that pathway might include the following.

Step One: The buy in. Management and advisors team to encourage the board to fully embrace cybersecurity as a governance oversight responsibility. This may include sharing with the board the new NACD guidelines. The message must be clear that the issue is not so complex and technical as to outstrip the board's ability to exercise oversight, and that cybersecurity is not at the exclusive province of the CIO and his/her team. The board must be comfortable with the reasons why it is expected to add oversight, and what that oversight might contemplate.

---

[6] See e.g., Jeff Overley, "Big Year Ahead for HIPAA Fines, HHS Atty Says," Law360, June 12, 2014.
[7] See HHS Press Office, "HHS Requires California Medical Center to Protect Patients' Rights to Privacy," June 13, 2013 (*emphasis added*).
[8] 42 U.S.C. 1320d-5(d).
[9] Note that a data breach caused by a health system's outside revenue cycle vendor served as the basis for an extensive and highly public business practices investigation of a health system in 2012 by the state attorney general. As part of its settlement of litigation filed by the attorney general, the revenue cycle vendor accepted a six-year ban on doing business in the state.
[10] Martha Kessler, "Massachusetts Enforces Across Border As R.I. Hospital Settles Breach Notice Case," Bloomberg BNA, July 28, 2014.
[11] See e.g., Joseph Conn, "Advocate Beats Second Class-Action Suit, Faces Others over 2013 Data Breach," *Modern Healthcare*, July 14, 2014.
[12] Jason Green, "$4.1M Settlement Possible in Stanford Medical Information Breach," *San Jose Mercury News*, March 22, 2014.

Step Two: Education. The board needs to be "brought up to speed" concerning fundamental cyber issues as they present to the health system. This has an external component—a briefing on applicable laws (including related enforcement action) and recent risk-related developments (including examples of data breaches at hospitals and health systems). It also has an internal component—reviewing with the board the system's internal IT/data security hierarchy, the extent to which existing enterprise risk policies address computer security threat policies; prior organizational data and privacy concerns and other computer security issues; and how computer security issues have previously been addressed by governance, at the board and committee levels, and the information flow to governance on such issues.

Step Three: Forum. The board should consider whether a change needs to be made in the way cybersecurity oversight is currently practiced at the board level; is there a need for a more refined forum? Some boards choose to enhance computer security oversight by specifically assigning oversight to a new standing committee, to a current standing committee (e.g., audit or compliance), or the board as a whole (as many boards choose to address their enterprise risk management oversight responsibilities). There may also be value in directing greater internal coordination of cybersecurity matters at the board and management levels (e.g., committee to committee, executive to executive) to avoid a dangerous "silo effect." Board leadership may ask key officers (e.g., the compliance officer and the general counsel) to be more closely involved in the establishment of oversight protections and in providing board support on this issue. This may be particularly valuable given that much of the private litigation and regulatory enforcement actions include breach of duty allegations (i.e., that the data breach or similar computer security event was a direct result of the board's failure to implement and monitor an effective internal computer security risk management system).

Step Four: Competency. While board-level computer security expertise is not an absolute prerequisite for effective oversight, it surely can be helpful. For that reason, it may be helpful to include candidates with computer security background in the director nomination process. Computer security oversight is more likely to succeed with the presence of at least one subject matter expert on the board (or responsible committee).

Step Five: D&O coverage. Given the risk exposure involved, it is prudent for the board to work with the organization's general counsel to determine the extent to which existing indemnification and officer's and director's insurance policies provide protection to data breach-based legal actions asserting personal liability against board members.

Step Six: Board awareness. The ability of the board to exercise effective oversight will be aided by an understanding with the CEO and CIO on internal assignments; i.e., what matters are properly reserved to the CIO, what matters require board awareness, and what matters require board/committee oversight, action, and/or approval. (If the organization also has a chief privacy officer, that person should be included within this discussion.) An essential element of this would be an understanding on upstream risk reporting, and on what level of continuing board/committee education on computer security matters is necessary to support effective oversight. Part of this effort would include providing board-level support to the CIO; a new survey suggests that healthcare CIOs often bear a disproportionately high degree of responsibility for organizational data breaches.[13] Indeed, all executive-level employees should be encouraged by the board to support the CIO and the board in the implementation and operation of effective data security programs.

Conclusion

Well-run boards are protective of their agenda, and are aware of the risk that peripheral issues will serve as a distraction from matters that truly require the board's attention. Given that, it is understandable that cybersecurity may not have received a high-level focus by many hospital and health system boards. Those days are now over. There is overwhelming evidence suggesting that healthcare boards must adopt a more organized and concerted approach to matters of cybersecurity and data protection. Such an approach can be assisted by valuable guidelines prepared by organizations such as NACD, and should reflect a full appreciation for trends and current developments in the area. The general counsel, compliance officer, and the chief

[13] Joyce E. Cutler, "Chief Information Security Officers Viewed as Scapegoats in C-Suite Survey," *Corporate Law & Accountability Report*, Bloomberg BNA, August 2014.

information officer can be valuable participants with the chief executive officer in supporting board efforts to embrace more vigorous awareness of, and attention to, cyber risks.

The Governance Institute thanks Michael W. Peregrine, Esq., partner, and Edward G. Zacharias, partner, McDermott Will & Emery, LLP, for contributing this article. They can be reached at mperegrine@mwe.com and ezacharias@mwe.com.

■■■

The Rise of the Hospital Joint Venture

By Barry Sagraves, Juniper Advisory, and Ken Marlow, Waller

This article is the first in a series examining the advantages of joint ventures, the process of developing a joint venture, and expected trends related to these transactions.

Since the enactment of the Affordable Care Act in 2010, more and more hospitals and health systems have entered into some sort of affiliation, whether through acquisition, membership substitution, joint venture, or clinical affiliation. This trend is a result of the mounting pressures hospitals and health systems face in the current healthcare environment. Yet, fundamental change in the makeup of the hospital market also paves way for innovation, which includes new ways that organizations may partner to confront these challenges. The joint venture structure is one such innovation.

For those hospitals and health systems that are financially sound and have sufficient capital, entering into an affiliation allows them to best position themselves for future success—to thrive rather than just survive. Evaluating strategic alternatives from a position of strength allows the board of a hospital or health system to take its future into its own hands and identify affiliation partners that complement and enhance its operations, capitalization, compliance, and quality functions. Exploring a range of joint venture alternatives has been found by many systems to be a "best of both worlds" approach—combining the installed market presence and reputation of a non-profit system with the scale, access to capital, and management expertise of an investor-owned company.

Most hospital and health system boards are aware of the trend of consolidation; however, many fail to appreciate the full range of strategic alternatives that may exist (including the joint venture structure) and the processes and tactics that can identify and realize the board's desired outcomes. This article is the first in a series in which we will examine 1) the potential advantages of joint ventures; 2) how to go about the process of exploring a joint venture, including selecting a joint venture partner; and 3) expected trends and future developments with joint ventures.

Challenges Posed by Industry Changes	Emerging Opportunities
• Reimbursement cuts year over year • Increasing costs and expenses for information technology in connection with electronic health records, meaningful use, and collection of data for quality metrics comparison, all key elements of successfully managing population health • The requirement for effective compliance programs and, in the event of noncompliance, being subjected to repayments, penalties, and other sanctions • Increasing challenges in financing capital expenditures, and continuing or increasing pension funding challenges	• Vertical integration, where health systems may vie to "control the premium dollar" rather than being a price taker from insurance companies • New ways of developing and sharing clinical protocols to reduce variation in outcomes and improve quality • Make capital investment decisions on a regional basis, across all elements of the health system

Advantages of Joint Ventures

Hospitals and health systems are looking to joint ventures for a number of reasons, many that are common but others that may be unique to potential partners. Some of the most common factors are:

- **Governance**: One of the key areas that many boards find attractive about joint ventures is that the current organization remains an owner and is directly involved in the governance of the venture. While gaining access to increased capital and opportunities, the local board remains very much "at the table" in managing the organization. There is, however, no standard model among potential partners, and both the legal structure and the day-to-day realities of decision making must be carefully explored and negotiated.
- **Investment potential**: A second potential advantage in a typical non-profit/investor-owned joint venture is that the non-profit corporation retains an equity stake in the business, which it will expect to increase in value over time. In addition, as a charitable organization, it will be able to diversify its holdings with the sale of an interest in its current business, reducing its overall portfolio risk.
- **Access to capital**: The capital needs of a hospital or health system are extraordinary. A hospital that enters into a joint venture has the benefit of additional sources of capital. A financially healthy partner can share the burden of capital investments, whether for working capital, routine, or strategic capital projects. Even with a fairly healthy financial position, many organizations find themselves facing limits to their debt capacity or significantly underfunded pension plans. These liabilities can often be eliminated as part of the joint venture transaction.
- **Enhancement of quality**: In the evolving healthcare environment, the hospitals that provide the best quality of care will be rewarded, while those that do not meet the requisite standards will face consequences. Specifically, the Affordable Care Act includes a value-based purchasing program, which rewards hospitals that exceed quality measures and penalizes underperformers with payment cuts. Partners that have a history and reputation of clinical and quality excellence, as well as access to highly specialized medical services, will provide the assistance to ensure not only that patients are receiving the best quality of care, but also that, as a result, the hospital is rewarded financially for providing excellent care.
- **Physician recruitment, retention, and alignment**: Another way a joint venture can strengthen a hospital or health system is through physician recruitment and retention. Partners that have strong physician networks and a proven ability to attract and retain physicians will continue to be critically important to the success of a hospital. Partners that can provide resources to aid physicians and caregivers in skills development and career plan development of staff at all levels of the organization will be attractive to hospitals. In addition, investments in a significant infrastructure of recruiting, the sourcing of specialists and practice management experts, and support for promoting practices and retaining quality physicians will be instrumental in ensuring success. A final, psychological point cannot be underestimated: physicians, particularly in an employment situation, want to "join a winner" that can offer them the potential for a secure professional and financial future.
- **Efficiencies and bargaining leverage**: With the implementation of the Affordable Care Act, the cost of doing business has increased, while reimbursement has decreased. This has placed increased pressure on hospitals and health systems to find efficiencies and engage in cost-cutting efforts. Through joint ventures, healthcare organizations can find synergies in various aspects of the operations, such as back office, management, and administrative functions. They also may have more leverage in negotiations with suppliers and payers. In addition, the larger scale may provide for better terms with respect to health and welfare benefits, as well as insurance policies.
- **Continuation and expansion of services**: The continuation and expansion of healthcare services is critical to the success of hospitals and health systems. A joint venture with a strong partner can solidify the ability of the organization to provide existing services and in many cases provide additional specialty services that are not currently offered at the hospital. With the addition of a joint venture partner, the hospital also may be better positioned to offer additional ancillary services, such as diagnostic, laboratory, and pharmacy services. By ensuring the continuation and expansion of services, the patient is more likely to seek care within the local community.

A Glossary of Hospital and Health System Transaction Structures

Below are the key structures seen in recent partnerships announced by hospitals and health systems:

- **Seller joint venture**: Seller joint ventures (SJVs) are typically, but not always, formed between a community hospital and an investor-owned company. The investor-owned company acquires a majority interest in the hospital (usually 60–80 percent). However, local control is preserved for the community via 50 percent hospital representation on the joint venture board. In these arrangements, the hospital gains access to needed capital while maintaining a collaborative culture, and the investor reaps returns if and when the hospital partner grows its market share. *Example: LHP Hospital Group's joint venture with Portneuf Medical Center in Idaho.*
- **Buyer joint venture**: Buyer joint ventures (BJVs) combine the respective expertise of a clinical partner or a system with a regional presence with an investor-owned system. The clinical partner holds a minority of the equity interest (typically 3–20 percent) and is responsible for overseeing medical safety and quality or providing regional services. The investor-owned partner provides capital (typically 80–97 percent), management capabilities, and economies of scale to run the community hospital. These partnerships have been very successful and appealing in recent years. Together, the BJV goes out to acquire hospitals and health systems. *Example: Duke LifePoint's joint venture that acquired Conemaugh Health System in Pennsylvania.*
- **Shelf joint venture**: In order to be ready to compete effectively for acquisition opportunities, it may be advisable to structure the BJV before there is an actual target available. Typically a letter of intent is signed between the prospective joint venture partners, which is then made binding simultaneously with the closing of the acquisition. A shelf joint venture is a strategy for forming a partnership in advance of a partnership opportunity.
- **Consolidation transaction**: A consolidation occurs when two parties combine to create a new parent company with a self-perpetuating board. Consolidation transactions are difficult to execute but typically double the size of the individual partners, quickly achieving scale. This was a very popular structure in the 1990s and has seen a revival post-health reform. *Examples: Advocate Health Care in Chicago, Banner Health in Phoenix, and Sentara Healthcare in Virginia.*
- **Membership substitution**: A membership substitution is the most common structure between merging non-profit hospital systems. The seller transfers its membership to the non-profit acquirer, which becomes the new "owner." The structure is used in non-profit transactions where the seller wants its corporate structure to remain intact post-closing, or the buyer wants to assume, rather than retire, the liabilities. *Example: Meriter Health System joining UnityPoint Health.*
- **Asset sale**: The typical structure for an investor-owned acquisition of a non-profit. The buyer acquires the assets (working capital, fixed assets, intangibles) and excludes most liabilities, which the seller then retires. Remaining funds are used to establish a local community foundation that can be used for various charitable purposes, including promotion of healthcare in the community. *Examples: Sale of Marquette General Health System to Duke LifePoint and sale of Guthrie Medical Center to Mercy Health.*

Note: For a more in-depth look at the various structures, see Jordan Shields and Rex Burgdorfer, "The Expanding Range of Strategic Alternatives in Hospital System Mergers and Acquisitions," *BoardRoom Press* Special Section, Vol. 25, No. 4, The Governance Institute, August 2014.

Conclusion

Hospitals and health systems across the nation are faced with challenges unlike ever before. We have provided here a brief overview of the advantages that many hospitals are finding in joint ventures and other affiliations. In our next articles, we will further discuss how a hospital board should go about developing a joint venture and other models, the trends we're seeing, and what we predict to occur in the months and years to come.

The Governance Institute thanks Barry Sagraves, managing director at Juniper Advisory, and Ken Marlow, partner at Waller, for contributing this article. *They can be reached at bsagraves@juniperadvisory.com and ken.marlow@wallerlaw.com. Juniper Advisory is an independent investment banking firm dedicated to providing its hospital industry clients with M&A and other strategic financial advice. Waller is a law firm specializing in healthcare transactions and regulations.*

■■■

New Publications and Resources

Episode 4: Analytics in Population Health (PopCity DVD, September 2014)

Strategic Cost Transformation for Post-Reform Success (White Paper, Summer 2014)

BoardRoom Press, Volume 25, No. 4 (*BoardRoom Press*, August 2014)

The Board's Role following the Wave of Industry Consolidation (E-Briefings Article Series, July 2014)

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

Upcoming Events

Leadership Conference
The Greenbrier
White Sulphur Springs,
West Virginia
October 19–22, 2014

Leadership Conference
The Ritz-Carlton, Naples
Naples, Florida
January 18–21, 2015

Leadership Conference
Boca Raton Resort & Club
Boca Raton, Florida
February 22–25, 2015

Click here to view the complete programs and register for these and other 2014 and 2015 conferences.

■■■