FYA For Your Advantage

An Essential Tool for Healthcare Leaders

Sponsored by PHNS Innovative Solutions to Complex Problems

Volume 8, Issue 13 - July 6, 2009

From TrendLeader Connections

FYA* - For Your Advantage**, is a free twice-monthly electronic newsletter. With every issue, ***FYA provides insights into the topics that concern healthcare leaders today and the challenges they will face in the near future. The newsletter is provided free to healthcare CEOs. The editorial content is not copyrighted – except for those columns copyrighted by the author. CEOs may use the non-copyrighted material in any way they wish. The newsletter can be printed without prior permission.

***FYA* - For Your Advantage** is produced by **TrendLeader Connections**. TLC offers a variety of healthcare products and services that help executives to differentiate between "fads" and "trends" and to make connections with "Trend Leaders" within the healthcare industry.

Table of Contents

***FYA* Staff**

Publisher Jerry F. Pogue
Editor S. Harvey Price
Web Master Joel Schlarb
Circulation Manager Sheila Keizer

TrendLeader Connections
26 Shawnee Way, Suite C
Bozeman, MT 59715
(406) 586-6400

We Won't Take Control of Healthcare by Rearranging the Deck Chairs On the Titanic

By John W. Kenagy, MD, MPA

Health industry leaders recently told the Obama administration that we can improve quality and lower the cost of care by simplifying and reducing administrative costs, making hospitals more efficient, reducing hospitalizations, managing chronic illnesses more effectively and improving healthcare information technology.

So how will it happen? As a physician, healthcare executive, academic scholar, advisor, author, and most importantly, a patient, I have watched us attempt to achieve those objectives by doing the same things in the same ways over and over again for more than 40 years: gathering data; holding lots of meetings; analyzing, planning and predicting; implementing solutions with experts, consultants, committees, task forces and technology; and then aligning incentives and holding people accountable on the frontline.

Now we are repeating the process. As Yogi Berra said, "It's déjà vu all over again!"

We are not going to succeed by trying harder with 1978 methods. I propose the root cause of our problem is that we are saddled with an antiquated management approach better designed for mid 20th Century factories than 21st Century healthcare. Trying harder will deliver exactly what it has already delivered – less care at higher cost. We are not in control.

Trying harder is simply rearranging a few more deck chairs on the Titanic – it might improve the appearance of the healthcare ship, but it will continue to leak and it will inevitably sink. The recent announcement of the eminent insolvency of Medicare Part B suggests our Titanic is taking on water a lot faster than we anticipated and we have a limited number of very antiquated lifeboats with which to save ourselves.

The organizations who will save the ship will be led by those who, as Peter Drucker said, "accept what we all know is elemental – that taking a defensive position can, at best, only eliminate losses. And we need gains." Trying harder is a defensive position. We need gains. We need to take control and work differently.

Fortunately, there is a simple set of principles for taking control, building more lifeboats and eventually constructing a much better healthcare ship.

Principle #1 – You start to gain control when you recognize that your future success is not dependent on what you have done in the past or are doing now, but rather on how you adapt what you are doing to a constantly changing environment. If you don't adapt, you lose control; it's as simple as that.

Principle #2 – Understand that the structures and systems of your current organization and the habits, behaviors and values of the people embedded within it will always slow, stall and often stop adaptive change. This is an organizational fact of life proven by Harvard Business School Professor Clayton Christensen in his concept of disruptive innovation. Most of us have experienced it. You increase your control by understanding that your organization's previous success will be part of the problem. As General Motors discovered, what got you here, not only won't get you there, it gets in the way.

Principle #3 – Develop the internal capability to continuously adapt. Organizations that are strategically and operationally "designed to adapt" have incredible competitive advantage in a rapidly changing world. They are in control. They will rebuild the ship over and over again.

(Continued...)

We Won't Take Control of Healthcare by Rearranging the Deck Chairs On the Titanic (Continued...)

Christensen says it is almost impossible for an established organization to lead adaptive/disruptive change. But, if it's "almost impossible," that means it's possible. In my four years as a Visiting Scholar at Harvard Business School, I studied the small number of companies who excelled at adapting to complex, dynamic, unpredictable work and found recurrent patterns of success in taking control.

I took those successful methods and then tested, validated and improved them in the crucible of frontline healthcare. Working with organizations like Mayo Health System, Ascension Health and Palomar Pomerado Health, we've created methods, skills and tools that allow healthcare's management and frontline to deliver on the fundamental promise of our calling – getting patients exactly what they need at continually lower cost.

The formula is called Adaptive Design® – designed to get healthcare back to the ideals of patient care by cultivating adaptability in the everyday work of everyone. It delivers control by creating healthcare that is "designed to adapt."

My forthcoming book, *Designed to Adapt: Leading Healthcare in Challenging Times* (Second River Healthcare Press, 2009), tells what healthcare leaders can do to regain control. The solutions are not complicated, just different.

It explains how management starts to increase control not by moving more data and information up to decision makers, but rather by developing and coordinating critical thinking skills and decisions right where the information is – in the workplace.

The method for making this transition is well documented and deceptively simple, but runs counter to current managerial expectations. To take control, you don't gather data, call meetings and think about it. You act. You do. You can't *think* your way into a new way of acting; you *act* your way to a new way of thinking. You take control.

The key to taking action safely is to use the "three M's" – **make** change, **maximize** the effects of change that are positive and **minimize** the effects of change that are negative. As consultants, my associates and I have tested and validated the following steps that have delivered the "three M's" in numerous organizations. We are now ready to support your management team in leading this work and taking control from the start.

Here's what the process looks like:

1. Identify a place in your organization, as close to the patient as possible, to be your first learning laboratory and innovation incubator.
2. Focus this unit – from the CEO to the frontline – on getting patients exactly what he or she needs at continually lower cost.
3. Equip staff, physicians and management with the skills and tools needed to identify circumstances when a patient does not get exactly what he or she needs and empower them to solve the problem immediately in the course of work.
4. Use Adaptive Design discipline and structure to rigorously create, test, validate and spread the solutions.
5. Be relentless and opportunistic in developing the knowledge and creativity of everyone in your organization to replicate what works as rapidly as possible.

It's fast, simple and safe. Set direction, identify and problem solve when systems fail. Replicate what works.

What taking control does not mean is repeating our 40-year old habit of gathering more data, having more meetings and implementing more big solutions. Taking control means changing the business case for healthcare. I will guarantee the successful organizations of the 21st Century will:

1. Excel at return on assets rather than try to make a return on investment
2. Regenerate capital rather than access and expend capital
3. Innovate with ingenuity rather than technology
4. Create new best practices rather than copy someone else's best practice
5. Develop people, not things, as their organization's # 1 resource

This time, rather than rearranging the deck chairs on the Titanic, take control and make sure that *everyone is empowered* and *everyone is accountable* to take the lead in adapting his or her corner of the organization to any and all new realities.

For healthcare, leading in challenging times means taking control and revitalizing trust, optimism, high performance and innovation that makes a difference for patients. Take control by getting patients exactly what they need at continually lower cost. It's the way to fix healthcare. Make it everyone's job. Otherwise, we will all go down with the ship.

Contact Dr. Kenagy at jkenagy@kenagyassociates.com

FYA For Your Advantage
An Essential Tool for Healthcare Leaders
Sponsored by PHNS Innovative Solutions to Complex Problems

"Meaningful Use" Melee

By Rick Kneipper, Chief Administrative Officer and Co-Founder of PHNS

A veritable flood of industry comments showed up by the June 26, 2009 deadline in response to the request for public comment regarding the definition of "meaningful use" of "certified EHR technology" that was proposed by the Office of the National Coordinator for Health Information Technology ("ONC") on June 16, 2009.

The ONC asked for "stakeholder feedback" regarding whether its proposed definition was "overly aggressive based on the current state of technology and the demands on new provider workflows, or not challenging enough..." The ONC proposed that "meaningful use" be defined to include a series of technologies that would "improve quality, safety, efficiency and reduce health disparities," as mandated by Congress when it allocated over $30+ billion of stimulus monies to improve healthcare IT. However, it appears that a significant number of industry commentators think that the ONC was overly aggressive:

- The **American Medical Association** and over 80 other physician groups commented that the ONC's "timeline to meet the proposed measures is too aggressive given that we continue to lack the necessary infrastructure, standards and systems;"
- The **American Hospital Association** said that "the proposed sequence for adoption is overly aggressive and unrealistic for most" and instead urged that ONC adopt a definition that "begins with fewer functional requirements and extends the transition to a fully functional EHR beyond 2015," stating that "Our members….consider a 2011 Computerized Provider Order Entry (CPOE) requirement to be unrealistic;"
- The **Health Information and Management Systems Society** said that the CPOE requirements should be delayed from 2011 to 2013, as it had previously recommended; and requested more clear distinctions between requirements for hospitals and those for physician practices;
- The **College of Healthcare Information Management Executives** suggested that the ONC require that a specific number of the 55 functions proposed by the ONC be adopted each year from 2011 to 2014, rather than setting forth specific functions to be adopted by specific years;
- The **Association of Medical Directors of Information Systems** stated that the ONC's CPOE requirement should be deferred from 2011 to 2013 since "Implementing full CPOE is an important but complicated undertaking fraught with potential unintended negative consequences if done too quickly or incorrectly," but it did state that "Ambulatory e-prescribing is a notable CPOE exception that we are comfortable recommending for 2011 because it is a mature enough technology to be reasonably considered 'ready for prime time' and will have a sufficiently impactful effect on quality and cost to be worth striving for." It also recommended that quality measures be deferred until 2013 when it believes data capture and sharing will be in widespread use; and
- The **American Health Information Management Association** suggested that a requirement to provide clinical summaries for patients for each encounter may need to be delayed from 2011 to 2013 and recommended some specific definitions for CPOE, but did not urge a delay in the CPOE requirements.

All of these comments raise valid concerns. However, the ONC must find a way to balance the "go slow" recommendations from industry with the clear Congressional mandate that the stimulus monies should only be used to improve patient care and quality, which we all know has not improved significantly since the Institute of Medicine told us in 1999 that about 100,000 were dying each year from medical errors.

Unless the ONC raises the bar significantly, the $30+ billion of stimulus monies will be spent to buy and implement more of the technologies we already have in our hospitals.

This generally does not help to improve patient care and quality according to many physicians, nurses and other clinicians and according to important studies by well-regarded independent groups such as the National Research Council, the Center for American Progress and the Markle Foundation.

Our U.S. patients (aka. taxpayers) want and deserve more, and there are numerous examples of innovative hospitals and physicians who have developed or found technologies and processes that have significantly improved patient care and quality – we can and should do better than using stimulus dollars to fund more of the status quo.

I would like to hear your comments.
Send them to:
Richard.Kneipper@phns.com

Your Money or Your Life

The late comedian, Jack Benny, could not have known that someday a famous line from one of his skits would apply to healthcare. One of the major challenges of reforming healthcare is its costs.

Inflation in our healthcare system remains the most important and difficult part of reform. According to a poll by *The Economist* magazine, cost is a tender nerve: 61 percent thought the high cost of care and insurance was a bigger problem than the number of uninsured, against 31 percent who believed the reverse. Only 21 percent would be willing to support a reform plan if they had to pay more in insurance or tax; 62 percent would not.

Some of the blame is not entirely justified. One blame is price gouging by drug companies. In fact, pills account for barely a tenth of healthcare spending in America and similarly small shares elsewhere. But aren't costs lower in Europe because of price controls? Europe does indeed spend less on new branded drugs, but also uses fewer generic drugs and pays much more for them. And Switzerland actually has higher drug prices than America (as does Canada). "Greedy drug makers" are not the main cause of America's runaway costs.

Nor are baby-boomers, though they are often blamed for healthcare inflation because there are a lot of them and they are getting old. Ageing will clearly push up costs in time, but it is not the main culprit yet. The Congressional Budget Office estimates that ageing accounts for only a quarter of the healthcare inflation to come in the next few decades, and the share in other rich countries is similar.

Doctors' generous pay is another popular culprit. But doctors in several European countries are well paid too. The Organization for Economic Cooperation and Development (OECD) estimates that general practitioners in America earn 3.7 times the average wage. Their British counterparts earn 4.2 times their national average. American specialists earn 5.6 times the average wage, against 7.6 times for their Dutch colleagues. Yet healthcare costs in Britain and the Netherlands remain lower than America's. The real problem is not how much American doctors are paid, but how. The system of medical reimbursement warps incentives for doctors, insurers and patients that lead Americans to consume more and more medical services. There is strong evidence that Americans use pills, procedures, scans and other expensive forms of healthcare more often than do patients in other rich countries, and not always to good effect.

America's insurance system encourages overuse in several ways. One is the tax break that favors health insurance provided by employers, which leads to excessively generous coverage and hence over-consumption. Another is the fact that American health insurers earn a lot of revenue from administering the health plans provided to employees by big corporations which, in effect, insure themselves. This leaves insurers with no incentive to curb costs, because more spending means fatter management fees.

The incentives facing doctors are even more perverse. Most doctors are not paid a fixed salary, still less rewarded for better health outcomes. Integrated American systems such as Kaiser Permanente and the Mayo Clinic are exceptions to this rule, and Britain's National Health Service is trying to adopt a similar approach. But most doctors and hospitals are paid more if they provide more services, regardless of the results. Predictably, this leads to far higher rates of doctors' visits, specialist referrals and scans.

For instance, the OECD countries have an average of 11 MRI machines per one million people. America has 25.9. America uses them more often, too: 91.2 times per 1,000 people per year, compared with the OECD average of 39.1.

This incentive problem even extends to patients. If patients pay very little out of their own pockets they have little desire to curb consumption. Though this is a problem in many OECD countries, in America the proportion of out-of-pocket spending has declined sharply in the past few decades. And a new report by McKinsey, a management consultant firm, identifies a more subtle problem. Having examined insurance and out-of-pocket spending for several health risks, it concludes that Americans are generally "over-insured and under-served." It is prudent for individuals to have comprehensive health insurance against catastrophic health risks such as heart attacks or cancer. But McKinsey finds that Americans with private health insurance often have generous coverage for non-essential and even medically unjustified care. This encourages over-consumption.

Reform won't be easy in our country.

Data Privacy and Network Security Risk: Is Your Facility Prepared?

By Tom Green and Sylvia Brown

Data breaches and attacks that reveal personally identifiable information and financial data are on the rise. Since January 2005, more than 260 million data records have been exposed, with an estimated 35.6 million records exposed in 2008; 7.3 million of these were healthcare records.[1] Of the personally identifiable information exposed, 211,655 instances involved paper records, and the overwhelming majority of exposures, approximately 7.1 million, originated in electronic data.

Despite the numbers, many healthcare organizations still make excuses when confronting cyber liability issues. Typically, businesses assume: a) this will not happen to them; b) they are covered under existing property or liability insurance; c) their systems are secure; and/or d) they cannot afford the expense of insuring against this problem. This faulty logic does not take into account the overwhelming costs of a security breach, from legal fees to lost business.

Another cost to consider in the event of a data breach is that of notification. Beginning with the July 2003 enactment of the California Security Breach Information Act, 44 states have passed laws requiring companies storing personal information to promptly notify people whose information may have been accessed by an unauthorized person. Should prompt notification not be provided, civil liability can result.

Think your records are secure? Consider the following case where a remark from one employee revealed inappropriate patient information and cost one hospital dearly. A New York State Appellate Court recently upheld a $365,000 jury award against a healthcare center that mistakenly disclosed information regarding a patient's medical information. A subsequent phone call, based on this information, revealed the patient's abortion to her mother. The court held that the plaintiff could be awarded punitive damages for an unintentional breach of confidential medical information even if there was no malice or malicious behavior by the defendant.

As this example illustrates, the clichéd image of computer hackers breaking into systems is far from the only way personal health information is exposed. The most common types of breaches include:

- Lost or stolen laptops, computers or other computer storage devices
- Employees stealing information or allowing access to information
- Viruses, trojan horses and computer security loopholes
- Internal security failures
- Backup tapes lost in transit because they were not sent either electronically or with a human escort
- Information bought by a fake business
- Poor business practices
- Improper disposition of information (paper and electronic)

The variety of breaches noted above proves that despite having the best defense in place, a security failure could happen to any hospital. The average cost of a data breach is $202 per lost customer record, with a $6.65 million average total cost per breach. Of that, $4.55 million, or $139 per record, is attributed to lost business. The other $2.1 million, or $63 per record, is comprised of costs associated with internal investigation, attorneys, customer notification, call center support, crisis management and media, credit monitoring and regulatory investigation defense. These figures emphasize the need to obtain supplemental insurance protection against a large potential financial loss to an organization that suffers a data breach.

If you are not yet convinced that the risk of not protecting sensitive patient information does not outweigh the associated costs, consider the implementation of new regulations under the North American Free Trade Agreement (NAFTA) Red Flag and Address Discrepancy Rule Compliance. The regulation requires creditors to develop and implement a written plan for detecting, preventing and mitigating identity theft. These regulations are applicable to most hospitals and healthcare providers deemed as creditors. As a result, hospitals and other medical care providers must adopt and implement a broad identity theft prevention system as of August 1, 2009.

Requirements for implementation of the NAFTA regulations include approval by a Board of Directors or governing body with continual oversight in development, implementation and administration; training staff and implementing new methods; and annual reporting to the Board of Directors including identified incidents and program effectiveness.

Additional new regulations are on the horizon in the form of the Health Information Technology for Economic and Clinical Health (HITECH) Act, recently signed into law as part of the widely publicized American Recovery and Reinvestment Act (ARRA). HITECH allocates approximately $20 billion to promote healthcare IT through investment in IT infrastructure to support a national health information network, development of related standards and financial incentives for physicians and hospitals to help them acquire and implement electronic health records. This immense infusion of capital and technological resources is intended to increase the use of EMR and thus facilitate patient care.

(Continued...)

Data Privacy and Network Security Risk: Is Your Facility Prepared? (Continued...)

The HITECH Act also augments and significantly strengthens HIPAA privacy requirements. For example, the act establishes data breach notification requirements for HIPAA covered entities and business associates, requiring notification of individuals whose unsecured protected health information (PHI) has been accessed or disclosed as a result of a breach. While regulations further defining a breach are still being drafted, the law specifies that it is an "unauthorized" acquisition or access of "unsecured" PHI, which is generally interpreted to mean "non-encrypted." The definition of a breach does not usually include unintentional acquisition by an employee. Nevertheless, once a breach has been committed, the act requires that notice be provided to the affected individual(s) by one or more of the following methods:

- Written notice by first class mail or as specified by the individual
- If insufficient contact information exists, post on home page of Web site of covered entity or notice in print or broadcast media
- Notice to HHS of breaches affecting more than 500 individuals
- Notice to prominent media outlets if PHI of more than 500 individuals are affected

With the rise of data breaches and new pending legislation, hospitals cannot afford to ignore security issues. The following are recommendations for steps to take now:

- Be familiar with HITECH provisions and stay apprised of HITECH regulations as they are issued. As appropriate, take advantage of the pertinent regulatory comment period.
- Review existing privacy and security mechanisms to be sure they meet current HIPAA requirements, as significant new "tiered" civil penalties for noncompliance became effective in February 2009.
- Identify external vendors with access to your PHI data.
- Review security procedures used by business associates (third parties handling PHI as part of their relationship with a healthcare organization).
- Implement an incident response policy which includes breach notification.
- Establish procedures for dealing with breaches.
- Identify systems containing PHI data.
- Consider the purchase of cyber liability insurance which provides coverage for data breaches.

Most importantly, talk with your organization's risk manager as you formulate strategies to address data privacy, an exposure with increasingly significant ramifications.

Tom Green, ARM, CIC, is Senior Director of Sales & Marketing at Premier Insurance Management Services, Inc. in Charlotte, NC. Tom can be reached at tom_green@premierinc.com.

Sylvia Brown, RN, JD, is Director of Risk Management at Premier Insurance Management Services, Inc. in San Diego, CA. Sylvia can be reached at sylvia_brown@premierinc.com.

Tom Green, ARM, CIC

Sylvia Brown, RN, JD

References:

1. Identity Theft Resource Center 2008 Data Breach Statistics