BoardRoom Press

A Bimonthly Journal of News, Resources, and Events for Today's Healthcare Boards

THE GOVERNANCE INSTITUTE ■ VOLUME 28, NUMBER 6 ■ DECEMBER 2017
GovernanceInstitute.com

THE GOVERNANCE INSTITUTE

A SERVICE OF nrc HEALTH

Alignment of Governance and Leadership in Healthcare: Building a Roadmap to Transformation

Social Media and the DNA of Healthcare

SPECIAL SECTION

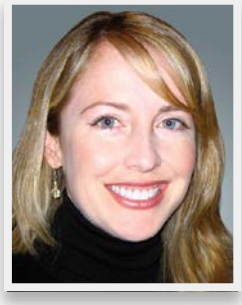
Myths and Fallacies of Computer Security in Healthcare Environments

Physician Burnout: What Next?

ADVISORS' CORNER

Navigating Strategic Uncertainties: The Board's Role

Looking Ahead to the New Year



Another tumultuous year in healthcare is coming to an end, without any more clarity (in fact, less!) about federal legislation. We are still riding the uncertainty tide and are likely to continue well into the new year. Does this hinder our progress to transform our organizations into value-based population health delivery models?

What we do know is that most of the uncertainty lies in how the insurance market will change. How payers pay for care has huge implications for hospital revenues, of course. But the need to increase healthcare value in the U.S. continues to increase. Let's focus on transforming care delivery to be smarter, better, less costly, and more efficient. We need hospital and health system boards that are also smarter and more efficient to lead this charge. We need more and faster movement in this direction.

Some critical issues facing healthcare boards in this regard are covered in this issue, including addressing the drivers of poor health in our communities, protecting our organizations and patient data from cyber attacks, the increasing concern regarding physician burnout and how to deal with it, using social media as a strategic tool, and finally to close the loop, learning how to navigate strategic uncertainties. It's been quite a year, and we look forward to new challenges and opportunities in the new year. We hope this year of *BoardRoom Press* has been a vital resource to your board, and we welcome your feedback!

Kathryn C. Peisert

Kathryn C. Peisert, *Managing Editor*

Contents

3 **Alignment of Governance and Leadership in Healthcare: Building a Roadmap to Transformation**

4 **Social Media and the DNA of Healthcare**

5 SPECIAL SECTION
Myths and Fallacies of Computer Security in Healthcare Environments

13 **Physician Burnout: What Next?**

16 ADVISORS' CORNER
Navigating Strategic Uncertainties: The Board's Role

THE GOVERNANCE INSTITUTE

A SERVICE OF nrc HEALTH

The Governance Institute®
The essential resource for governance knowledge and solutions®

9685 Via Excelencia • Suite 100
San Diego, CA 92126
Toll Free (877) 712-8778 • **Fax** (858) 909-0813
GovernanceInstitute.com

/TheGovernanceInstitute
/thegovinstitute

The *BoardRoom Press* is published six times a year by The Governance Institute. Leading in the field of healthcare governance since 1986, The Governance Institute provides trusted, independent information, resources, and tools to board members, healthcare executives, and physician leaders in support of their efforts to lead and govern their organizations. For more information about our services, please call toll free at (877) 712-8778, or visit our Web site at GovernanceInstitute.com.

EDUCATION CALENDAR

Mark your calendar for these upcoming Governance Institute conferences. For more information, please call toll free (877) 712-8778.

LEADERSHIP CONFERENCE
The Ritz-Carlton, Naples
Naples, Florida
January 14–17, 2018

LEADERSHIP CONFERENCE
Fort Lauderdale Marriott
Harbor Beach Resort & Spa
Fort Lauderdale, Florida
February 18–21, 2018

LEADERSHIP CONFERENCE
Fairmont Scottsdale Princess
Scottsdale, Arizona
March 11–14, 2018

Please note: Conference expenses paid for by a board member can be claimed as a donation and listed as an itemized deduction on the board member's income tax return. Please consult your tax advisor for more information.

Alignment of Governance and Leadership in Healthcare: Building a Roadmap to Transformation

BY KEVIN BARNETT, DR.P.H., M.C.P., AND STEPHANIE SARIO, M.SC., PUBLIC HEALTH INSTITUTE

The Challenge

Today's healthcare leaders are confronted with a plethora of complex, time-sensitive demands for decisions in new and unfamiliar areas, and in a policy environment that is uncertain at best. The imperative for meaningful change is countered by resistance from powerful forces, both internal and external, and growing demands for capital expenditures at a time when financial margins are narrowing.

Kevin Barnett, Dr.P.H., M.C.P.
Senior Investigator,
Public Health Institute

Stephanie Sario, M.Sc.
Program Manager,
Public Health Institute

Investments in new data systems are confounded by resistance from physicians, resentful that time with patients is limited by increasing demands for data entry and handoffs to new and unfamiliar team members. Building a more comprehensive picture of patient populations through application of analytic methods and data sharing across organizations is impeded by proprietary concerns, as well as design inconsistencies driven by the profit motives of data technology firms. The focus on quality of care in clinical settings is complicated by the growing recognition that most of what drives the health of our patients is in the external world and outside our control. Our hospitals are increasingly expected to assume financial risk for reducing the demand for acute care medical services for specific populations, when the bulk of financial rewards are for filling beds and conducting procedures. These challenges are particularly acute for safety net hospitals with high percentages of low-income populations who reside in socially and economically disadvantaged communities.

While a growing number of hospital and health system leaders recognize the need for bold decisions, they report to a board of directors whose competencies and orientation are still driven primarily by the legacy focus on fiduciary stability. Gaining their support for actions that move beyond legacy concerns requires both education and a deeper form of engagement; one in which their input informs strategic decisions as healthcare organizations become involved in improving health and well-being in communities.

Key Board Takeaways

It is now crucial that hospitals and health systems become more involved in improving the health and well-being of the communities they serve. A few steps boards can take include:

1. Allocate substantial time (e.g., two to three hours) for board education and deeper examination of the impact of the social determinants of health.
2. Build shared knowledge of variations in health status and quality of life among residents in surrounding communities (e.g., differential prevalence and acuity for chronic diseases and service utilization patterns by race, ethnicity, and geography).
3. Review board competencies and expand to encompass skills needed to support deeper engagement across sectors in regional markets. (In the process, you may discover the presence of invaluable skills you didn't know were present!)
4. Establish protocols for board meetings that create space for in-depth dialogue by sharing materials ahead of time and limiting presentations.
5. Join us for a future AGLH intensive!

The Opportunity

For the last 18 months, The Governance Institute, in partnership with the Public Health Institute and Stakeholder Health, has led the Alignment of Governance and Leadership in Healthcare program (AGLH). AGLH is an initiative funded by the Robert Wood Johnson Foundation that focuses explicitly on building shared knowledge among senior leaders and board members to better address the drivers of poor health in communities. Stakeholder Health is a collaborative partnership of health systems from across the country whose leaders share a commitment to build genuine partnerships with diverse community stakeholders to address the drivers of poor health. The Public Health Institute is a private nonprofit organization with a long history of supporting the advancement of community health improvement practices through partnerships among hospitals and community stakeholders across the country.

To date, the AGLH program has brought together teams and individual representatives of over 75 hospitals and health systems, ranging from large national systems and their subsidiaries and multi-facility regional systems, to urban academic health centers, and stand-alone rural hospitals. Examples of national systems and their subsidiaries that have participated include Catholic Health Initiatives, Trinity Health, and Ascension. Regional systems range from UMass Memorial Health Care and University of Vermont Medical Center, to Mountain States Health Alliance and Wake Forest Baptist Medical Center. These and others invested in two-day intensives that combined presentations and dialogue with thought leaders with team work sessions that provide an opportunity to drill down into how new knowledge may be applied in diverse settings.

The Experience

AGLH faculty are current or former hospital and health system CEOs, board members, and other senior leaders who share their direct experience in the application of innovations and lessons they've learned in the process.

Participant teams are supported in the completion of a self-assessment tool that assists in determining the relative progress of their organizations in areas such as data systems development, care redesign, financial innovations, and integration of community benefit and population health management. The intent is to create a safe space for senior leaders and board members to move beyond generalized discussions to a deeper examination of structures, functions, and progress to date.

Teams have responded positively to the experience, particularly the opportunity

continued on page 14

Social Media and the DNA of Healthcare

BY LEE AASE, MAYO CLINIC SOCIAL MEDIA NETWORK

Since the dawn of human history, social networking has helped people recover from illness. Through word-of-mouth they learned about folk remedies, and as science progressed and medicine became more useful, our ancestors increasingly sought treatment from doctors reputed to have successful track records, having learned about them from their satisfied (and surviving) patients.

Doctors likewise participated in analog social networking, traveling to observe others and eventually forming scientific associations where they would gather to present case studies. This eventually led to peer-reviewed publishing of research and development of guidelines and best practices.

This is the history of medicine in general, and of Mayo Clinic in particular. As the sons of Dr. William Worrall Mayo joined his practice in Rochester, Minnesota in the 1880s, it was the dawn of a golden age of surgery. Improved anesthesia made complex internal operations possible, and aseptic surgical techniques meant more patients survived to tell their stories.

The railroad and telegraph caused news of the surgical exploits of William J. Mayo, M.D., and his brother Charles H. Mayo, M.D., to spread rapidly. Soon the railroad began bringing patients from as far as New York and Montana, and upon their return home the word-of-mouth radius continued to grow.

Dr. Will and Dr. Charlie, as they became known, were committed to learning from others, studying surgery in every town in the U.S. and Canada with populations of more than 100,000, as well as 25 countries from Australia and Argentina to Russia and Sweden. This travel was all by train and steamship, which further highlights their commitment to outreach and learning.

The brothers also welcomed physicians to Rochester to learn from them. Between 1908 and 1918, nearly 3,400 visiting physicians became members of The Surgeons Club, the informal association of those who had observed the Mayo brothers.

This history of old-fashioned, face-to-face social networking explains why Mayo Clinic was an early adopter of modern social media platforms like Facebook, Twitter, and YouTube, and why we're also committed to helping our colleagues learn to use these tools safely and effectively.

We see social media not as radical inventions, but as natural extensions of the way humans have always communicated.

So do your employees and patients.

Facebook now has more than two billion monthly active users worldwide. Almost five billion YouTube videos are watched every day, and 6,000 tweets are posted to Twitter on average every second. Health and medical issues increasingly are part of these conversations.

How should hospital leaders and board members respond? Recognize that:

- **Non-involvement is not an option.** Most of your employees have social networking accounts. Your patients are talking about your hospital online. You will be affected by what they say, so you need to at least be listening. As marketing consultant Danny Brown noted, ROI has an additional meaning related to social media: risk of ignoring. Just as you would not dream of operating a hospital without a telephone number, you shouldn't be absent from social platforms where your patients expect to communicate.
- **Opportunities are amazing**. Direct involvement in social media gives your organization a voice, which your employees, patients, and other stakeholders can amplify. You can use these tools to streamline and improve the practice, too. A YouTube video, for example, could provide educational information to patients that physicians otherwise would present individually. That face-to-face time can be better spent answering specific questions prompted by the video.
- **Risks are real.** Social media platforms are the communications equivalent of power tools. A chainsaw can do work much more quickly than an axe, but also can do much more damage if used improperly. Likewise, social media allows positive word-of-mouth to spread farther and faster than face-to-face conversation, but also can expose confidentiality breaches to many more people.
- **Guidelines are necessary...** Your hospital probably doesn't need a separate social media policy, but you do need guidelines for your employees to interpret how all other policies apply in the social media sphere. We have published our Mayo Clinic employee guidelines as a model you can adapt.
- **...But without employee training, guidelines are insufficient.** Strong guidelines poorly communicated and then enforced with a "gotcha" spirit do not contribute to a positive culture. Regular communication and training will help staff embrace social media opportunities with confidence.

continued on page 14

Key Board Takeaways

Below are some tips for how hospital and health system boards can effectively apply social media tools in their organizations:

- Because of their prevalence in society, social media will affect every hospital, regardless of size, as employees and patients will be participating in these platforms.
- Hospitals should create employee guidelines and training programs so employees understand how organization policies apply in social media. Effective guidelines and training can help hospitals realize the benefits of social media while mitigating risks.
- Social media should not be considered in isolation, but integrated with other communication and marketing tools.
- Free templates and resources to aid in strategic planning and guideline development are available through the Mayo Clinic Social Media Network (MCSMN), at https://socialmedia.mayoclinic.org.

Myths and Fallacies of Computer Security in Healthcare Environments

BY SEAN PEISERT, PH.D., LAWRENCE BERKELEY NATIONAL LABORATORY

The U.K. National Health Service (NHS), U.S. Office of Personnel Management (OPM), Experian, Sony, the Democratic National Committee, the Republican National Committee, the U.S. Department of Health and Human Services, Yahoo, Anthem, Premera Blue Cross, 21st Century Oncology, Banner Health.

Anyone reading this probably recognizes each of these organizations as a few of the dozens that have reported a cyber attack in recent years, such as ransomware or a database breach, and a few of the hundreds or thousands that have been the victim of damaging attacks but did not report it, and/or had one but failed to find one.

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

If the more well-resourced cyber attackers in the world, such as nation states, wanted to attack your organization, they could likely find a way to do so successfully. In the same fashion, should tanks roll up to the front door of your organization, they could probably find a way to get inside. On the other hand, most cyber attacks are not the equivalent of tanks rolling up to your front doorstep, but are much more often the equivalent of street muggings. In any case, there is no reason organizations should make it easy for such attackers.

Thus, there are three vital tenets for healthcare board members to keep in mind about computer security:

1. Security *is* your organization's responsibility. You have a responsibility to your employees, your customers, and patients, and much as is the case with public health, to your "neighbors"—the other organizations you interact with.
2. The security situation is *not* hopeless.
3. There is no such thing as "perfect" security. Your organization will *not* prevent all attacks. Some will succeed. What your organization needs to do is figure out how to architect its security program so that, when attacks are successful, the damage is limited.

In this special section, we discuss common misconceptions about security, ways in which organizations can try to succeed, and what boards need to know about security.

Mitigation

Conventional Wisdom and Compliance

"To be secure, here's what you need to do: install a firewall; have your employees make strong passwords of at least 12 characters, composed of upper and lowercase letters, numbers, and symbols, and change their passwords every six months; pay for a security monitoring system; install anti-virus scanners on all your computers; and put your employees through annual security training."

This is the kind of advice one might expect to hear from a computer security consultant. Some of these things *might* help, but there is also good evidence that some of these things produce no value or may even be counter-productive. Consider recent advice from the Federal Trade Commission:

> "...there is a lot of evidence to suggest that users who are required to change their passwords frequently select weaker passwords to begin with, and then change them in predictable ways that attackers can guess easily. Unless there is reason to believe a password has been compromised or shared, requiring regular password changes may actually do more harm than good in some cases. (And even if a password

Key Board Takeaways

There is no such thing as "perfect" security—it is impossible to prevent all attacks. Healthcare organizations need to architect their security programs so that, when attacks are successful, the damage is limited and recovery is swift. Moreover, security is an ongoing, continuous effort. The following are some key issues and questions for board members to consider:

1. Merely following the herd by using so-called "best practices" is no longer defensible. "Compliance" with regulations (e.g., HIPAA and HITECH) is *not* the same thing as true "security."
2. Security staff should regularly analyze potential points of vulnerability. Often those most vulnerable points are employees' desktop computers. Could some workers complete their tasks using more secure devices such as those that run on Apple's iOS or Google's Chrome OS? In addition, scenario planning must be robust so that, in the event of a breach, steps can be taken immediately to identify and remedy the problem.
3. Questions for board members to ask the CIO and CISO include:
   - » Are we storing the right amount of data in order to make meaningful decisions and actions related to patient care, or are we storing data we are not using?
   - » Once we have looked at the data, how long do we need to keep historical data?
   - » Are we properly destroying old data that is no longer required?
4. Emphasize bi-directional communication between the people who make decisions about security (e.g., the CISO's team) and the rest of the organization. Security is everyone's responsibility.
5. If you are running your own servers and backups, ensure there are multiple tiers/locations of data storage, and consider expanding to cloud provider solutions.
6. Don't go it alone, but don't blindly rely on vendors or consultants and consider the job done. Seek out other organizations in your region that have strong security infrastructure, or are seeking solutions as well, and share strategies, best practices, and lessons learned. Consider the possibility of creating an alliance of organizations that can build a unified security infrastructure with shared resources.

has been compromised, changing the password may be ineffective, especially if other steps aren't taken to correct security problems.)"[1]

Others cite similar issues:

- "...None of the common recommendations that user passwords should be long, strong, contain certain characters, kept unique to each account, never written down, and changed regularly appears to be supported.... While numerous organizations give password guidance, none that we can find supports them with evidence of improved outcomes..."[2]
- "This week, Google security researcher Tavis Ormandy announced that he'd found numerous critical vulnerabilities in Symantec's entire suite of anti-virus products. That's 17 Symantec enterprise products in all, and eight Norton consumer and small-business products. The worst thing about Symantec's woes? They're just the latest in a long string of serious vulnerabilities uncovered in security software."[3]
- "Department of Defense data (cleared for release) shows on average one-third of vulnerabilities in government systems is in the security software."[4]

So, rotating passwords and installing security software may actually make your organization *more* vulnerable? It is important to note that proper authentication is *vital*, as is the use of certain types of security software. But what if the solution to malware isn't installing virus scanners, but in broadening the use of devices that are more "locked down" and less "open" than traditional desktop PCs? As an analogy, the solution to surviving a tornado may not be the world's fastest car that can outrun tornados, along with sensors that can provide

real-time wind speed, but rather may well be a traditional U.S. Midwestern basement.

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

To that end, it should come as little surprise that security experts are finding that endpoints such as those based on Apple's iOS or Google's Chrome OS are often more secure[5] than endpoints running traditional desktop operating systems, such as Microsoft's Windows. Tim Cook, the CEO of Apple, has indicated that an iPad, not a Mac, is his primary work machine.[6] How many people who live in Microsoft Word, Excel, PowerPoint, and Outlook could instead do just fine with Chrome OS?[7] How many people who are doing primarily Internet research could similarly use a Chrome OS device or iPad? A question from the board to your organization's Chief Information Officer might be: could some of our workers complete their tasks using more secure devices such as those that run on Apple's iOS or Google's Chrome OS?

The answer to security training is similarly nuanced. Security training of employees *can* improve results.[8] However, "beyond a certain threshold, increasing demands [on users] are simply met with attempts to circumvent onerous procedures. The thresholds appear to have been long exceeded for most users."[9]

This critique is not to say that conventional wisdom should be stopped

1 Lorrie Cranor, "Time to Rethink Mandatory Password Changes," Federal Trade Commission, March 2, 2016 (www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes).
2 Cormac Herley, "Unfalsifiability of Security Claims," *Proceedings of the National Academy of Sciences,* Vol. 113, No. 23 (2016), pp. 6415–6420, available at www.pnas.org/content/113/23/6415.
3 Kim Zetter, "Symantec's Woes Expose the Antivirus Industry's Security Gaps," *Wired,* June 30, 2016, available at www.wired.com/2016/06/symantecs-woes-expose-antivirus-software-security-gaps/.
4 Mudge (Peter Zatko), "DoD data (cleared for release) shows on average 1/3 of vulns in government systems is in the security software," September 12, 2015 (twitter.com/dotmudge/status/642758829697056768?lang=en).
5 Rich Mogull, "Tidal Forces: The Trends Tearing Apart Security As We Know It," January 3, 2017 (https://securosis.com/blog/tidal-forces-the-trends-tearing-apart-security-as-we-know-it); and Rich Mogull, "Tidal Forces: Endpoints Are Different—More Secure, and Less Open," January 18, 2017 (https://securosis.com/blog/tidal-forces-endpoints-are-different-more-secure-and-less-open).
6 Jake Smith, "Tim Cook: 80 percent to 90 percent of my time is spent on an iPad, working and consuming," *9to5Mac,* February 14, 2012; Adrian Weckler, "Tim Cook: Apple won't create 'converged' MacBook and iPad," *Independent.ie*, November 15, 2015 (www.independent.ie/business/technology/tim-cook-apple-wont-create-converged-macbook-and-ipad-34201986.html).
7 Google Chromebooks (www.google.com/chromebook/).
8 Iacovos Kirlappos and M. Angela Sasse, "Security education against phishing: A modest proposal for a major rethink," *IEEE Security & Privacy*, Vol. 10, No. 2 (2012), pp. 24–32.
9 Adam Beautement, M. Angela Sasse, and Mike Wonham, "The Compliance Budget: Managing Security Behavior in Organizations," *Proceedings of the 2008 New Security Paradigms Workshop (NSPW),* September 2008, pp. 47–58; and Cormac Herley, "More is Not the Answer," *IEEE Security & Privacy,* Vol. 12, No. 1, 2014.

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

The HIPAA Security Rule[10] underlies most of the techniques that are used in healthcare to protect patient health information (PHI). However, the HIPAA Security Rule itself is rather high-level and non-prescriptive. This is probably intentional, because the rule must apply equally to organizations of any size and capability and therefore must target the lowest common denominator. The guidance from the National Institute of Standards and Trust (NIST) on HIPAA[11] is significantly more detailed, but still out of reach of many organizations. On the flipside, DHHS's "Security Standards: Implementation for the Small Provider"[12] provides so little detail as to enable "small providers" to do little more than "check the box" about being in compliance with the HIPAA Security Rule, which, as we've discussed, is *not* the same thing as true security. Take note that being in compliance with the HIPAA Security Rule may help a medical organization in a federal audit, but it does nothing to help with the confidence of the public and patients in the event of a breach. In the event of such a breach, for every minute of downtime, the worried public will be wondering if their own heath might be impacted by the failure. Boards should ask their Chief Information Security Officer if there has been scenario planning analysis to examine the potential impact to their systems in the event of a breach due to an unknown vulnerability, and what the steps might be to minimize the damage and restore operation.

Finally, thus far, we've spoken primarily about PHI and the HIPAA Security Rule, and not at all about medical sensors and devices. It is important to note that the same denial-of-service attacks that were unleashed in late 2016 by malware installed on so called "Internet of Things" devices such as remote cameras and network-connected baby monitors could easily have been installed on network-connected patient ventilators, MRI systems, radiation machines, computer-controlled drug dispensing machines, and more. Indeed, it is worth noting that one of the earliest catastrophes causing loss of life due to a computer controlled system was due to a radiation therapy machine, the Therac-25, which gave massive overdoses of radiation to at least six people[13]—and that error was due only to a bug in the software that was accidentally triggered, and not due to an intentional attack.

Challenging Conventional Wisdom

In contrast, therefore, to advice from a security consultant, this is the kind of general insight that executives and boards actually need to hear:

- "Software is the most complex thing made by humans…. [Developing software] is like having to assemble a bridge starting from subatomic particles, and you're not allowed to use the current laws of physics as a reference.[14]
- "Data is a toxic asset."[15]
- "Behavioral data: Don't collect it. If you have to collect it, don't store it. If you have to store it, don't store it long."[16]
- "It is a *fantasy* to think that our current security methods have any chance of protecting [critical] systems…. This fantasy is protected and promoted by an elaborate and pernicious mythology based solely on existing practice."[17]

However, if this set of advice is really what healthcare executives and boards need to hear, what should they do, as a result? After all, if data is a "toxic asset," what should a medical institution do, since patient data is an essential aspect of providing medical care? Unlike other organizations that collect data more or less indiscriminately—consider the department store that installs beacons around the store to monitor the Bluetooth signals emanating from customers smartphones to track their movement through the store, or the Web site that tracks every purchase a customer makes in order to send targeted ads to them—a hospital collects patient data for the express

10 U.S. Department of Health and Human Services (HHS), HIPAA Security Rule (www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/).
11 U.S. Department of Health and Human Services (HHS), HIPAA Security Rule Guidance, July 14, 2010 (www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf).
12 U.S. Department of Health and Human Services (HHS), HHS Security Standards: Implementation for the Small Provider, December 10, 2007 (www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf).
13 Nancy G. Leveson and Clark S. Turner, "An Investigation of the Therac-25 Accidents," *Computer,* Vol. 26, No. 7 (1993), pp. 18–41.
14 John Siracusa, "Accidental Tech Podcast," Episode 56, March 14, 2014 (atp.fm/episodes/56-the-woodpecker).
15 Bruce Schneier, "Data Is a Toxic Asset" (blog), March 4, 2016 (www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html).
16 Pinboard, Twitter post, November 11, 2016 (twitter.com/Pinboard/status/797169153194889218).
17 Sean Peisert, Ed Talbot, and Matt Bishop, "Turtles All the Way Down: A Clean-Slate, Ground-Up, First-Principles Approach to Secure Systems," in *Proceedings of the 2012 New Security Paradigms Workshop (NSPW),* pp. 15–26, Bertinoro, Italy, September 19–21, 2012.

We interviewed Neil Gomes, Chief Digital Officer and Senior Vice President for Technology Innovation and Consumer Experience at Thomas Jefferson University and Jefferson Health to get his perspective on how Jefferson is building cybersecurity infrastructure and ongoing strategies for maintaining security in a rapidly growing academic health system. He also serves on advisory boards for IBM and Adobe and is in the Google Next Leaders Circle.

The Governance Institute (TGI): *Where and how are you focusing efforts right now related to cybersecurity?*

Neil Gomes (NG): The primary challenge facing Jefferson is joining disparate health systems with different processes, networks, protocols, and training. Once infrastructure is addressed, security is first a human problem. So our first efforts have been focused around training and simulations; getting people to better understand what they should or shouldn't send via email, what phishing scams look like, when in doubt don't click, and so forth.

Another education focus is of our own IT employees. For example, with the WannaCry issue, if everyone had installed the patch, it would have been fine. But when a patch is released it needs to be vetted because we run a lot of complex systems like FAA code and EMR, or business process applications and financial applications. Some of them don't work if you apply these patches. They could break the interfaces or the functioning of certain software, so you have to test. Some of it is manual. Some of it is automated. Some of it is your relationship with the vendors providing you with other applications that could be affected. We are hiring security analysts so we can accelerate the process of vetting these types of solutions that come onto our network or patches that need to be applied, and do that in a much faster way.

Then in the innovation space, there's a lot happening in machine running where we can establish baseline activity and then start looking at hotspots of sudden activity on the network—the ability to identify sudden increases in activity, either around an application or a type of process that's happening, that could be an indicator of some kind of inappropriate activity on the network. Once the system senses a potential issue, we can orchestrate multiple sets of automated processes that run to either contain the threat or alert people that something is going on.

These threats come up so often that you cannot rely on manual security analysts to find these things on your network, or react in an analog kind of manner. You need to orchestrate and automatize.

TGI: *Are HIPAA compliance and using the HITRUST framework secure enough, or do you feel it's important to go further?*

NG: I think it's important to go further because those regulations many times are set in place to deal with the bare minimum but to real risk to the organization. These are lessons we learned when we went through this process. We have a huge responsibility to our own patients. They trust us with our data. Some of the vendors walk away from us because they can't meet our requirements. It also ensures that the vendor has some skin in the game.

TGI: *What advice do you have for other organizations that might not have the same degree of capability as Jefferson or need to outsource security?*

NG: If you do everything in-house, you first have to purchase all the software and hardware, even before you start using it. That's a high cost burden. Then you also have to hire very talented security professionals. And your ability to hire someone who is better than someone at Google is probably lower because Google has the attractive brand and can afford to pay at a higher level. Slowly over time, Google and Amazon and other large cloud providers have commoditized the solution.

And most importantly, that's their business; it's not mine. My business is taking care of other people, saving lives. So I think it's a matter of being able to level with these types of companies. The commoditization is making the cost low. It's delivering it to you at the point of use. Google has over 750 security analysts and engineers, and they have skin in the game. So they're not going to risk their own reputation—they'll go way beyond what HIPAA or HITECH requires.

TGI: *From your perspective, what do you feel the board needs to know to feel ensured that the organization is doing what it needs to for cybersecurity?*

NG: The board needs reports on the current state and what the big problems are. They need us to ensure that at least we address the foundational issues. But beyond that I think there needs to be some structural question marks. For example, it is important to separate the functions of networking and security. They cannot be managed by the same people because if there's a security issue, often the problem lies with the networking team overlooking something. So if both teams are managed by the same people or group, the board is never going to realize the real problem. Another thing to look for is redundancy. An ideal redundancy is multi-tiered. If I'm storing my data with Google and my backup is also with Google, then that could be a problem. So you may want to have your redundancy services with a different cloud provider, and/or stored locally.

Secondly, IT staff should be running scenarios of what happens when a system goes down, and provide the board with some level of detail about plans in place to handle those scenarios. Suppose we get hit by a system lockout issue. How are we going to run through that whole scenario? If people start pointing to the same systems that could be affected, ask if those systems reside on the same server. I don't know if boards do really get involved in that. Boards generally ask for due diligence, but sometimes the problem is as simple as investing millions of dollars in something and then realizing you're relying on the same thing to get the whole network back up and running. There are vendors that will run simulations on your backup system to help determine possible scenarios and solutions.

Third, there is huge advantage in the cloud. If any proposal is presented to the board that doesn't involve some level of cloud in it, if it's all investment in local infrastructure, those systems are usually very proprietary and you'll run into problems and limitations.

Finally, especially with healthcare institutions, I think we should not be afraid of things we don't know. We owe that responsibility to our patients.

purpose of treating patients. And if our current security methods can't protect critical systems, what is the alternative?

For institutions—particularly academic medical centers that may already be familiar with everything in this piece—such organizations may have additional challenges of their own. These include not only patient records, but potentially also data and computing pertaining to medical research environments, such as the massive amounts of data being created by next-generation gene sequencers, and the analysis of that data. The solutions for securing such applications is not yet obvious, since as has been empirically demonstrated, traditional protection techniques, such as traditional firewalls are often not appropriate in such environments. To be sure, techniques are on the horizon—the "Science DMZ" network design pattern, which enabled "big data" network transfers for "open science" has led to the Medical Science DMZ.[18] And special-purpose computing chips can encrypt at higher rates than ever before. Cryptographic and statistical techniques to limit data exposure, such as fully homomorphic encryption, secure-multiparty encryption, and differential privacy are becoming realistic—the latter is now commonplace enough to be deployed by Apple and Google, for example. But "big data" in medicine, and the need for pooling and sharing that data to enable the kinds of research discoveries envisioned by the medical science community, is clearly a challenge of its own.

"No Silver Bullet"[19]

The reality is that there is no simple answer. But at the same time, as suggested earlier, the situation is not hopeless. Organizations must invest in security and take security seriously, even with the knowledge that no protection will be perfect. A set of questions from the board to the Chief Information Officer and Chief Information Security Officer might include:

1. Are we storing the right amount of data in order to make meaningful decisions and actions related to patient care, or are we storing data we are not using?
2. Once we have looked at the data, how long do we need to keep historical data?
3. Are we properly destroying old data that is no longer required?

Alternative Approaches

Don't Go It Alone

There is at least one truism for many organizations struggling to find a path forward: for most organizations, unless you are Google, Facebook, Microsoft, or Apple, or unless you are a major medical center with a very large IT budget and are located in a city rich with computer security talent, you probably should not try to solve the problem on your own. Organizations such as these are familiar with the HITRUST CSF[20] inside and out, and have large security programs with elements such as strong, multi-factor authentication, system hardening, backups, meaningful and appropriate training, and real-time network and system visibility. Incident response and recovery are well understood and integrated into the environment. These organizations probably already identified whether they need to run their own storage and email systems, and if each of their personnel needs a full system running Windows, or whether Google Apps and Chromebooks will do.[21] If this describes your organization, you have a massive head start on doing "all the right things."

Outsourcing and Consultants May Not Be the Answer

However, most healthcare organizations may have only pieces of this, and a budget to enable hiring the right team to put all of this in place in a way that is truly effective, rather than merely lip service to security, may be out of reach. On the other hand, outsourcing is not necessarily an effective solution, either. Consider the example of the Marin Healthcare District and Prima Medical Foundation whose patients were victims of a ransomware attack,[22] many of whose medical records were subsequently lost entirely due to an allegedly unrelated failure of the backup system.[23] These organizations *did* outsource, but did so to a small company that was not only incapable of blocking ransomware, which may well have been inevitable even for a more capable organization, but could not even maintain effective computer backups.

Healthcare executives and boards need to also keep in mind that not all computer security "experts" are created equal. While certifications from organizations such as

18 Sean Peisert et al., "The Medical Science DMZ: A Network Design Pattern for Data-Intensive Medical Science," *Journal of the American Medical Informatics Association (JAMIA),* 2017 (DOI: 10.1093/jamia/ocx104; https://academic.oup.com/jamia/article/doi/10.1093/jamia/ocx104/4367749/The-medical-science-DMZ-a-network-design-pattern).

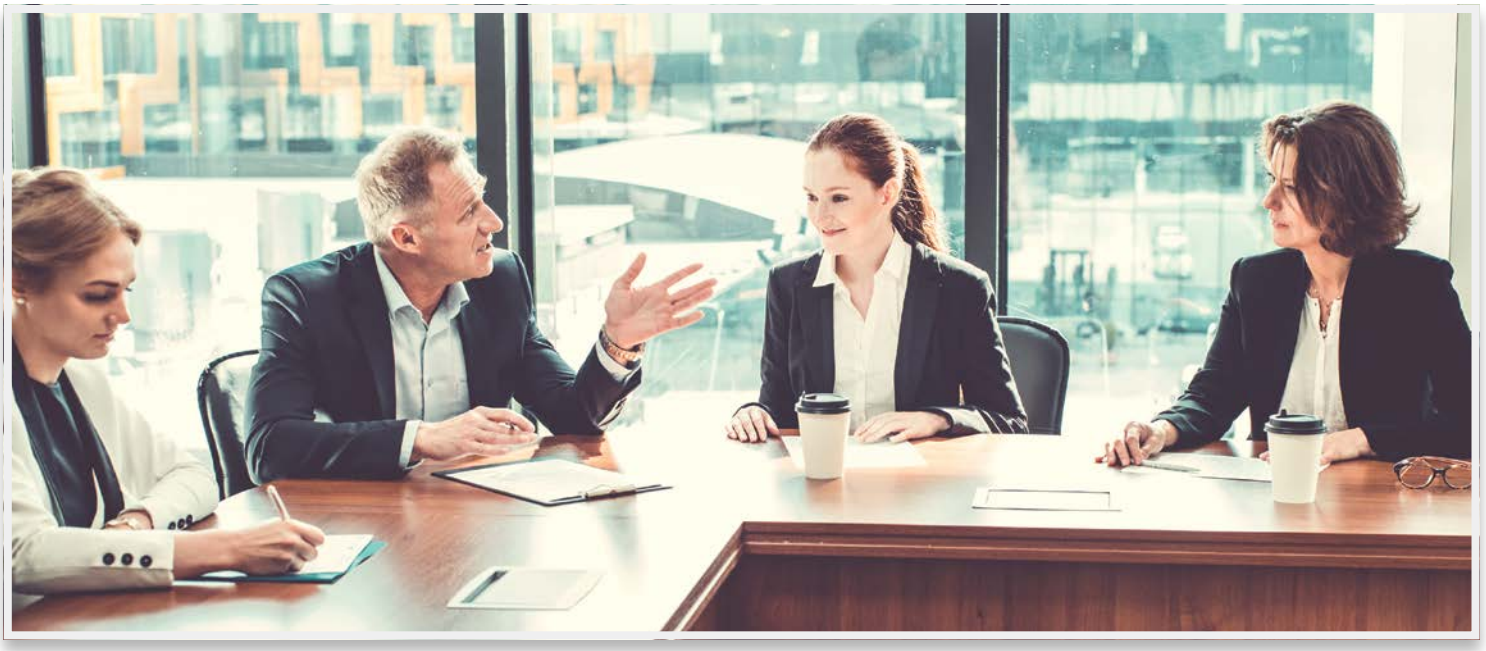
19 Fred P. Brooks, "No Silver Bullet—Essence and Accidents of Software Engineering," *IEEE Computer,* Vol. 20, April 1987, pp. 10–19.

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

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

22 Richard Halstead, "Marin electronic medical record system hacked, ransom paid," *Marin Independent Journal*, August 4, 2016.

23 Richard Halstead, "Marin patients' medical data lost after cyber attack," *Marin Independent Journal*, September 29, 2016.



the SANS Institute's "Global Information Assurance Certification (GIAC)" and the International Information System Security Certification Consortium's "Certified Information Systems Security Professional (CISSP)" exist to provide a base level of competence in certain activities pertaining to computer security, and serve useful purposes, true excellence in leadership pertaining to computer security, including both in-house, top-flight chief information security officers and security engineering talent, are extremely rare. But that is what is needed, rather than consultants who parachute in to stand up a token security program and then depart until there is an incident to recover from. The consequence, of course, is that trusting a large part of a modern medical institution's lifeblood—patient data and, increasingly, network-connected medical instruments—to anyone less than top-flight talent is a Las Vegas gamble.

In the very short term, hiring a security consultant to come in to assess risk and implement mitigations is one option. Organizations such as the HITRUST Alliance may be able to help find such a person. This should not be considered the end of the problem, but rather a starting place. Finding the "right" consultant is not an easy task. There is no reliable set of criteria that would distinguish a consultant who is not only generally qualified, but has sufficient abilities to understand the distinctive aspects of your organization, in order to understand and implement the risk mitigation mechanisms. And further, consultants, by definition, are typically adjunct to the organization, and come in to do something and then leave. In contrast, security must be continuous, ongoing, and deeply ingrained. In my opinion, the most effective approach for the long term is for organizations to partner together to work on common, secure infrastructure, practices, and procedures that are both broadly effective *and* broadly implementable. A "lowest common denominator" implementation that only reaches the "compliance" bar is no longer a viable option.

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

—Sean Peisert, Ph.D.

Consider the actions after the 4.5-million patient breach at the UCLA Health System[24] and the two breaches at UC Berkeley resulting in the theft of 80,000 employee records[25]—the University of California instituted a system-wide "threat detection and identification approach" covering all 10 campuses and five academic medical centers to obtain consistency of practice, economies of scale, and leverage the limited pool of top security talent across the entire

24 Chad Terhune, "UCLA Health System data breach affects 4.5 million patients," *The Los Angeles Times*, July 17, 2015.
25 Dave Lewis, "University of California Berkeley breached again," *CSO*, February 27, 2016.

system.[26] All of a sudden, the entire University of California is more or less able to be one of the types of organizations referred to earlier with "a very large IT budget and are located in a city rich with computer security talent."

Not every organization can implement something as extensive as the University of California has, with a combined, system-wide annual budget of nearly $30 billion and a president who was formerly Secretary of the U.S. Department of Homeland Security. However, it may be possible to form some kind of coalition with sufficient financial and personnel resources to bring solid capabilities.

How many organizations run their own email server? In contrast, how many organizations that *do* have cybersecurity talent choose to run their own mail server rather than leveraging Google's cloud services? Consider the many organizations, again, including the University of California, the U.S. Department of Defense, the U.S. Naval Academy, and the U.S. National Oceanic and Atmospheric Administration, who do the latter? The same thought process should apply to medical systems. Would the NHS ransomware attack[27] have been effective if the data had been stored in databases (compliant with U.K. health security and privacy laws) run by a major cloud provider? I think it is unlikely. The conclusion that one might draw from the decisions these organizations have made is that running one's own computing systems is often *not* the right idea if other organizations with extremely strong reputations may be able to do so more reliably, more securely, and at lower cost. (This is an example of outsourcing done right.)

> "My guess is that before long most processing of HIPAA data will be in cloud providers... imagine a world where there was a vetted architecture implemented by each of Google, Amazon, and Microsoft, with a safe harbor provision for use of technologies in approved ways."
>
> *—Eli Dart, Network Engineer, ESnet Science Engagement Group, Lawrence Berkeley National Laboratory*

Security Is the Responsibility of the Entire Organization

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

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

To build such a culture, the board should emphasize open, strong, and continuous bi-directional communication between the people who make decisions about security (e.g., the CISO's team) and the rest of the organization. In addition to the "core" security team composed of the CISO and security engineers and analysts, create a "virtual" security team of personnel from other parts of the organization, perhaps on a rotating basis, to join in weekly or bi-weekly security meetings as well.

Creating such a virtual security team enables personnel outside the core security team to learn more about the security challenges the entire organization faces, and to disseminate that knowledge to their peers. It also provides an opportunity for personnel outside the core security team to bring in fresh ideas and perspectives that the core security team may not have considered. This not only conveys information in both directions but helps align the motivations and goals of both sides—personnel outside the core security team better understand the needs of the security team, and the core security team better understands how other people in the organization need to be able to do their jobs.

A similar discussion between security staff and management is also vital. Many organizations have their CISO reporting to the CIO, or perhaps to someone even lower down in the organization. This can be a mistake, because frequent and bi-directional lines of communication between security and management, and indeed between security and the board of directors, are vital. Organizations with top security functions also tend to be organizations in which boards and management hear as regularly from security leads as they do from other business leads such as the CMO.

26 University of California Office of the President, "Purposes of a Systemwide TDI Approach," https://security.ucop.edu/services/threat-detection-and-identification/purposes.html.

27 Brian Krebs, "U.K. Hospitals Hit in Widespread Ransomware Attack," May 17, 2017 (https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/).

Conclusions

What should healthcare institutions do? First and foremost, it is vital that executives and boards learn to embrace security rather than resist it. Effective security need not be burdensome,[28] and can even be an *enabling* technology, not unlike how cleaning the oil filter in a car can do double duty for reducing emissions *and* making the car perform more responsively.

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

It's worth noting that there is some reason for optimism against all the bad news. For example, a community effort to create a "building code" for medical devices[29] has led to guidance issued by the U.S. Food and Drug Administration to produce more secure medical devices.[30] While the guidance is optional at this point, there is reason to be optimistic that the tide is turning. In addition, the rise of large "cloud" infrastructures also creates reason for optimism as well.

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

And, in many cases hospitals need no longer maintain as many traditional "computer systems" at all. There is almost a complete lack of malware that effects Apple's iOS operating system, for example, and unlike past arguments about the lack of malware affecting MacOS due to low market penetration, the same argument cannot be made about iOS. And the reason is not because of better "security software"—there is effectively none, or at least no anti-virus or traditional monitoring software[31]—but due to the ways in which iOS is more locked down and the iOS App Store has basic curation elements. To be sure, no one would claim that iOS is *secure*—no-non-trivial piece of software is. But it does appear to have key advantages. Given all this, what might a world look like in which data is largely stored on large, centrally monitored systems by professionals with experience comparable to those from the best companies and institutions in the U.S., and access to that data were mostly via highly-locked down iOS and other mobile devices?

The Governance Institute thanks Sean Peisert, Ph.D., Staff Scientist at Lawrence Berkeley National Laboratory, for contributing this special section. He is also an Adjunct Associate Professor of Computer Science at the University of California, Davis, where he does research and development in a broad cross-section of computer security, and teaches a course on security in health informatics at the UC Davis Medical School. He is also Chief Cybersecurity Strategist for CENIC, a non-profit organization that operates the network that provides Internet connectivity for over 20 million users in California, including the world's largest education system—the California K-12 system, California Community Colleges, the California State University system, California's Public Libraries, the University of California system, Stanford, Caltech, and USC, including the UC, Stanford, and USC medical centers and health systems. He received his Ph.D., Master's, and Bachelor's degrees in Computer Science from UC San Diego. He can be reached at sppeisert@lbl.gov.

28 Edward B. Talbot, Deborah Frincke, and Matt Bishop, "Demythifying Cybersecurity," *IEEE Security & Privacy*, Vol. 8, No. 3, pp. 56–59, May/June 2010.
29 Tom Haigh and Carl Landwehr, "Building Code for Medical Device Software Security," 2015 (cybersecurity.ieee.org/images/files/images/pdf/building-code-for-medica-device-software-security.pdf).
30 U.S. Food and Drug Administration, "Information for Healthcare Organizations about FDA's 'Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software,'" June 14, 2017 (www.fda.gov/RegulatoryInformation/Guidances/ucm070634.htm) and "Postmarket Management of Cybersecurity in Medical Devices—Guidance for Industry and Food and Drug Administration Staff," December 28, 2016 (www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf).
31 Rich Mogull, "Tidal Forces: Endpoints Are Different—More Secure, and Less Open," January 18, 2017 (https://securosis.com/blog/tidal-forces-endpoints-are-different-more-secure-and-less-open).

Physician Burnout: What Next?

BY LARRY R. MCEVOY, M.D., FACEP, PRACTICINGEXCELLENCE

The problem has become clear and ominous: by the end of 2014, 54 percent of physicians showed signs of burnout—chronic exhaustion, desensitization, cynicism—up from 45 percent just 36 months prior.[1] *One million* patients lose their physicians to suicide every year. "Physician, heal thyself" seems as appropriate—and inadequate—as ever. Somehow, we all—patients, doctors, organizations, and society alike—really need physicians *and* organizations to create an environment where physicians can stay healthy. In an industry where we have asked for more metaphorical honey—quality, efficiency, empathy, safety, innovation, responsiveness, value—from a committed swarm of very hard-working bees called doctors, the bees are starting to collapse, and with them the hive of healthcare.

"I was late to realize the magnitude of the problem, but I get its importance and impact now," one health system CEO recently told me ahead of a board retreat to address physician burnout. "I want this to be priority one." The medical literature on physician burnout has become more complete and continues to evolve, describing both the magnitude of the problem and emerging evidence that clarifies leverage points for action at the individual and organizational level,[2] in dimensions psychic, relational, and operational. Beyond the intrinsic unease about a nation of healing professionals being under such duress are clear and emerging impacts on patient experience, quality, safety, innovation, finance, and cost.

Burnout and Resilience—Fighting Words or Complementary Medicine?

Individual physicians cannot solve what has become a population epidemic, even if they find an individual hack to avoid their own burnout (e.g., reducing time at work, decreasing their time taking care of patients to stay personally healthy). Want to rub salt in the wound? Tell physicians in the face of withering stresses beyond their personal control, to practice resilience. Arousing particular rancor within physician ranks is the idea of practicing "resilience," as if "resilience deficit disorder" is driving physician burnout.

Burnout can be described as a chronic disequilibrium between stress and response. We need both stress and challenge, and healthy response patterns to shape our vigor and our performance. Too much stress, and it overwhelms anyone's capability to stay healthy; not enough capability to adapt, and we are overwhelmed even in the midst of "normal" stress. I like to think of burnout as personal and populational, helping us understand the origins and impact of a foundational challenge in the healthcare profession and industry. I think of resilience as systemic and strategic, pushing us to design operational, relational, and psychic dimensions of work to decrease stress and increase healthy responses at the individual, team, and organizational levels of the modern healthcare workplace. A burned out physician cannot outflank the withering pressures of the modern day clinical practice on his or her own. A resilient organization, however, focuses on both the stresses and the responses within its workflow processes, team dynamics, and individual support to decrease the likelihood of burnout, sharpen the focus for surveilling it, organize around the human and business reasons for preventing it, and allocate the resources for supporting those whose professional environments have become overwhelming.

A Population at Risk in a Stressed and Stressful Environment

As noted by Ariely and Lanier,[3] physicians are, as individuals and a population, at risk for burnout—we tend to focus on (and hear about) what hasn't gone well, by us and around us. We have a high need for autonomy and struggle when our days are filled with obligatory tasks mandated by distant and powerful forces, and we are always striving through varying forms of personal deprivation, for more. Personal and cultural traits of physicians aside, we live and work in professional environments that are "burnout inducing," that are correspondingly oppressive in what we have to do, must do, haven't done yet, and won't have time to do. These environments are nearly defined by the rewards asymmetry, loss of autonomy, and cognitive scarcity described by Ariely and Lanier—there is more negative feedback than positive, the focus is on compliance and obligation, and there is "never enough" time, FTEs, dollars, help, and support. The inspiring muses of serving humanity, collaborating with colleagues, and creating better ways to deliver care, can be hard to find. Doctors have been going without sleep, making critical decisions at pace, and multi-tasking for years—but today's healthcare work environment has become an unhealthy amalgam of medial

continued on page 15

Key Board Takeaways

Physician burnout is a major problem in the healthcare industry. Below are some key points for hospital and health system boards to be aware of, and some ideas for how they can work to solve this issue in their organizations:

- Physician burnout is an epidemic and omnipresent in the U.S. healthcare environment.
- Physician burnout represents the dysfunctional interplay between severe psychic and workflow stressors, and adaptive responses within healthcare organizations. While the stressors are falling disproportionately on physicians, they must be mitigated at other points in the healthcare system (i.e., simplicity of workflow design).
- Physician burnout compels redesign of the psychic, relational, and workflow parameters of any healthcare organization—it's both an urgent imperative and a redesign invitation.
- Boards and healthcare leaders have enormous obligation and opportunity to address this crisis and support a healthy physician population through familiarization with the causes of physician burnout, generative dialogue with physicians, redesign of the healthcare workplace, and monitoring of progress.

1 Tait D. Shanafelt et al., "Changes in Burnout and Satisfaction with Work-Life Balance in Physicians and the General US Working Population between 2011 and 2014," *Mayo Clinic Proceedings*, December 2015.
2 Colin P. West et al., "Interventions to prevent and reduce physician burnout: a systematic review and meta-analysis," *The Lancet*, September 2016.
3 Dan Ariely and William L. Lanier, "Disturbing Trends in Physician Burnout and Satisfaction With Work-Life Balance: Dealing With Malady Among the Nation's Healers," *Mayo Clinic Proceedings*, December 2015.

Alignment of Governance and Leadership…

continued from page 3

to engage board members in more of an exploratory, reflective exercise. A sampling of input shared by participants include:

- "The self-assessment tool was effective in getting us beyond a general conversation, and to focus on the infrastructure needed. It was an eye-opening experience."
- "The tool has helped to structure the strategic plan in a way that is helpful to our regional and local boards."
- "It generated important dialogue, forcing us to step back and say where we want to go. I don't think we've ever done anything like this before."

Participant teams also expressed strong support for a curriculum that focuses on how to engage boards and senior leaders in a deeper examination of their roles in working with others to address the drivers of poor health in communities. As stated by one board member, "What really struck me was setting the framework for how little we touch. There are a lot of others who have vital roles to play, and how do we integrate with them?"

Several senior leaders shared their initial trepidation about bringing board members into these kinds of discussions. Feedback since their participation suggests their courage to engage has been rewarded. As noted by one senior leader, "We have never had two days for a focused discussion on these issues, to immerse ourselves in it. The dialogue since then is on a much different level. It was very helpful to understand the impact of the social determinants of health, to really put it into our thought process more than it has been."

In addition to CEOs, CFOs, and other members of the senior leadership, many of the teams included vice presidents for population health. In some cases, these were recent appointments and their organizations are still determining how best to leverage the contributions of these new team members. Board members expressed their appreciation to spend quality time with senior staff that don't typically attend board meetings. As shared by one board member, "The intensive provided us with an opportunity to address key questions and have in-depth discussions about local/regional issues."

During the intensive, teams also completed an action plan that serves as a broad template for what kinds of potential next steps to take upon their return. The intent is to set a few targeted objectives, recognizing the need to share learnings and to engage a much larger contingent of organizational colleagues on the home front who did not participate in the intensive. Some teams indicated that they implemented the self-assessment tool with their full board and leadership.

Thanks to support from the Robert Wood Johnson Foundation, project staff conducted a series of six bi-monthly follow-up calls with many of the teams. In the process, they documented relevant accomplishments, challenges, and emerging lessons in the year after participation in the intensives. Most expressed strong support for continued engagement. As stated by one team member, "We appreciated the time to work together as a team, and the follow-up is critically important to add rigor and commitment that helps us move towards identified goals and objectives."

Next Steps

The support from the Robert Wood Johnson Foundation for the AGLH initiative clearly demonstrated the need for in-depth dialogue among senior leaders and board members on how to more strategically address the drivers of poor health in our communities. In the wake of the first three intensives, The Governance Institute has made a commitment to continue its partnership with Public Health Institute and Stakeholder Health in the immediate future. In a future article, we'll share details of the accomplishments, key challenges, and lessons reported by participating hospitals and health systems.

The Governance Institute thanks Kevin Barnett, Dr.P.H., M.C.P., Senior Investigator, Public Health Institute, and Stephanie Sario, M.Sc., Program Manager, Public Health Institute, for contributing this article. They can be reached at kevinpb@pacbell.net and ssario.phi@gmail.com.

Social Media and the DNA of Healthcare

continued from page 4

These recommendations apply to all organizations, from critical access hospitals, to academic medical centers, to hospital systems. How each will apply these tools will and should vary according to strategic priorities and organizational needs. Social media should not be considered in isolation, but as part of the communications continuum, and also as one element of the marketing mix.

Following in our founders' footsteps, in 2010 Mayo Clinic created MCSMN as an analog to The Surgeons Club for like-minded colleagues interested in applying social media to promote health, fight disease, and improve healthcare.

If Dr. Will Mayo would travel six weeks by train and steamship in 1924 to participate in a conference in New Zealand and visit surgeons in Australia, we have no doubt our founders also would have embraced these technologies that enable instantaneous communication.

You should too.

The Governance Institute thanks Lee Aase, Director, Mayo Clinic Social Media Network, for contributing this article. He can be reached at Aase.Lee@mayo.edu. The Mayo Clinic Social Media Network is a catalyst to accelerate safe and effective adoption of social media in clinical practice, education, and research. Access free resources, including guidelines and templates, at https://socialmedia.mayoclinic.org.

Physician Burnout: What Next?

continued from page 13

tasks, high risk, distraction, and alienation from the fundamental purpose and ethic of clinical care.

Is this just expensive after care? Probably not. Well-supported, energized physicians who can focus on the ethic of medicine, the healthy dynamics of their team in delivering and innovating care, and the strategic and operational fiber of their organizations (whatever they are), become an essential cohort for all the things we all need healthcare to be—more humane, more responsive, more efficient, more innovative, more cost-effective, more preventable, and more about individuals and populations. While some interventions will prove to be more effective than others, what is clear is that the scale and impact of the physician burnout epidemic calls for organizational redesign around sustainable approaches to performance, learning, and vitality, at all levels.

Is Physician Burnout Even Just about Physicians?

No. We are the current canary in the coal mine, but our healthcare population is full of burned out sub-populations from executives to nurses. Our societal patient population is sick, and our organizations are showing the stress and strain of an unsustainable burden of a stressed care system and distressful organizational processes and cultures. A commitment to simplicity, meaning, and supportive work communities will be critical to support the shifts in performance, structure, and innovation we all seek. If not, the physicians will probably keep trying, but they'll break down, leaving us with a growing doctor shortage and one million patients a year who lose their doctors to suicide.

What Can Boards and Leaders Do?

- Get educated—follow the literature and spend time listening to physicians, formally and informally.
- Think systemically—lead the organization in designing meaning, team culture, and workflow design in an integrated, focused fashion.
- Design and monitor at multiple levels—individuals, teams, and organizational processes impact and are impacted by each other. Before, during, and after initiation of organizational changes ask, "How does this action impact physician and team well-being, learning, and results?"
- Contribute to the growing body of literature on interventions that restore vitality in clinical populations.
- Make vitality and well-being a strategic and operational priority—prioritize them, resource them, and monitor them.

Physician burnout has emerged as a widespread red flag in the healthcare ecosystem, one which will persist into the foreseeable future. While research continues on how to understand and address this difficult challenge, boards and executives play a huge role in leveraging this issue to foster vitality, learning, and ultimately results, within their organizations. While large numbers of physicians struggle personally with the reality of burnout, the prevalence of the problem defines it as a strategic issue for every healthcare organization. Continued vigilance, learning, and action can help boards govern this issue with the priority and efficacy it commands.

The Governance Institute thanks Larry R. McEvoy, M.D., FACEP, Founder & Chief of Strategy & Innovation, PracticingExcellence, and Executive-in-Residence, Center for Creative Leadership for contributing this article. He can be reached at larry.mcevoy@practicingexcellence.com.

Navigating Strategic Uncertainties: The Board's Role

continued from page 16

members the opportunity to lead as well as govern.[3] Intrinsic to effective generative discussion is understanding that the fiduciary duty of loyalty does not expect or want board members to look only at the "good" of an organization; rather it requires members to put the best interests of the organization first. In today's dynamic environment, this means being willing to think about the uncomfortable.

Finally, the board should keep in mind this quote attributed to former General Electric CEO Jack Welch, "If the rate of change on the outside exceeds the rate of change on the inside, the end is near."[4] Your board's responsibility is to ensure that your leaders are unafraid to ask the right questions, are developing the right, adaptive culture, and are preparing the organization for success—even should the hurricane strike.

The Governance Institute thanks Marian C. Jennings, M.B.A., President, M. Jennings Consulting, Inc., and Governance Institute Advisor, for contributing this article. She can be reached at mjennings@mjenningsconsulting.com.

3 Peggy McGuire, "Generative Thinking: The Board's Highest Purpose," CompassPoint (blog), www.compasspoint.org/blog/generative-thinking-board%E2%80%99s-highest-purpose.

4 Jack Welch, "GE Annual Report, 2000," General Electric Company, February 9, 2001, www.ge.com/annual00/download/images/GEannual00.pdf.

Navigating Strategic Uncertainties: The Board's Role

BY MARIAN C. JENNINGS, M.B.A., M. JENNINGS CONSULTING, INC.

"If you live in Florida or Louisiana, you shouldn't spend a lot of time thinking about how likely it is that you'll be hit by a hurricane. Rather, you should think about what would happen to your organization if it was hit by one and how you would deal with the situation."[1]

Welcome to the bayou. This sage advice from a 2009 issue of *Harvard Business Review* was addressed to U.S. corporations facing the "storms" of severe market uncertainties and industry disruptors. How different might their futures have been if Sears, Blockbuster, and Toys"R"Us—among many others—had been more open to considering future scenarios that they hated to even acknowledge were possible?

This advice is especially relevant today for hospitals and health systems, given the many uncertainties and turbulence in our environment. Rather than debate exactly what changes will occur and when, hospital and system board members need to ensure that their organizations are adequately prepared for potential (albeit not certain) industry disruptions.

Articulate Uncertainties

An integral part of strategic planning is identifying "wild cards" or major changes in the market that would require fundamental changes in the business for continued success. The following are several examples of uncertainties from among the myriad ways our industry could be reshaped:

- **Payment**: If the U.S. moved to a single payer system or if Medicare were converted into a voucher system, what would be the impacts on your organization—and what should leaders be doing now to prepare?
- **Competition**: Will telemedicine and virtual health become the norm for primary care, specialty care, or both? What opportunities or challenges might this create?
- **New players**: Will Google, Apple, Intel, Facebook, or other consumer-savvy technology firms—with their seemingly unlimited resources—fundamentally alter how and where consumers seek care or "virtually" manage their own health? What could this mean for you?
- **Clinical breakthroughs**: What if there were a breakthrough to cure diabetes? Or new cancer treatments that would dramatically curtail demand for our traditional radiation therapy and chemotherapy programs?

Identify Potential Disruptors

Step one for your board, in concert with management, is to identify a short list of the greatest potential disruptors to your future success. This takes great courage, as it can be very scary to acknowledge that "hurricane force winds are out there." Be willing to name your worst-case scenarios and play devil's advocate against conventional wisdom. But remember, such disruptions should be plausible even if they are not likely.

Develop Scenarios/Contingency Plans

Step two is to identify contingency plans and "trigger points" associated with such disruptors. A solid contingency plan identifies the major actions that the organization would need to take should this industry disruption occur (akin to the disaster planning that you already undertake for local or regional physical disasters/disruptions).

"Trigger points" are like the canary in the coal mine: that is, they are early indicators of potential change. Leaders should identify and constantly monitor these trigger points. Federal payment changes, as an example, often can be foreseen years before they are enacted. Such predictable changes need not come as a surprise, although many hospitals and health systems scramble to adapt once implementation is imminent.

Promote an Adaptive Culture

Step three is for the board to enable and support an adaptive culture—that is, a culture with leaders who embrace change and are willing to take prudent risks, coupled with the systems and policies/procedures that support timely decision making. Culture starts at the top. The board itself must review its own processes and model the desired behaviors. Specifics for the board include:

- **Attract/develop new competencies on the board**: Ensure that the board includes individuals who have experienced rapid change in their own businesses, have demonstrated entrepreneurial skills, and can create consensus across stakeholders.
- **Update the CEO performance evaluation process**: Ensure that the CEO's performance expectations include indicators of effective performance and leadership in today's world as well as the ability to transform the organization for the future.[2]
- **Identify risks of both action and inaction**: Ensure that the board understands the financial, strategic, reputational, or internal political risks associated with being proactive. Equally important, ensure understanding of the risks associated with a "wait and see" approach.
- **Encourage open, candid discussion**: Board leaders should create a space for members to ask, "What problems may we be facing?" to gain insight into organizational identity and purpose. Often called generative discussion, this allows board

continued on page 15

Key Board Takeaways

The board cannot and should not be immobilized by the myriad uncertainties and turbulence in today's healthcare market. Taking a "wait and see" approach won't work during a period where stability is unlikely in the foreseeable future. Instead, we recommend that boards:

- Be courageous in facing up to the potential for significant market changes that could challenge your organization's strategies and/or continued success.
- Ensure that management has in place contingency plans for future scenarios that are plausible even if not currently likely.
- Actively support cultural changes, starting with the board's own processes that will increase your organization's agility and adaptability.

1 René M. Stulz, "Six Ways Companies Manage Risk," *Harvard Business Review,* March 2009.
2 Elements of Governance®: *CEO Performance Evaluation in the New Healthcare Industry,* Third Edition, The Governance Institute, 2016.