Colorado Trustee

For Colorado Hospital Governing Board Members
Spring 2014

GOVERNANCE INSIGHTS

Cybersecurity: A Growing Threat for Hospitals and Health Systems

Cybersecurity, sometimes referred to as “cyber attacks,” cost health care organizations billions of dollars each year. They put patients at risk, resulting in potential patient harm, hospital fines and penalties, and ultimately inflict serious consequences on an organization’s community trust and reputation. As stewards of the hospital’s financial health and representatives of the community’s interests, trustees must take the lead in ensuring that data security and patient privacy are a top priority at their organization.

According to Federal Bureau of Investigation (FBI) Director James B. Comey, the risk of cyber threats is growing, and “has become so dire that cybersecurity has topped the Director of National Intelligence list of global threats for the second consecutive year.” In his March 2014 statement, the FBI Director talked specifically about the risk in the health care sector, noting that health care spending consumes approximately 18 percent of the U.S. economy. Because of the prominent role it plays, health care is an attractive target for criminals. But, as Comey noted, it is not a victimless crime. Not only do cyber attacks result in increased costs for health care benefits, insurance, and taxpayers—they also have the potential to “cause actual patient harm, including subjecting patients to unnecessary treatment, providing sub-standard services and supplies, and passing potentially life-threatening diseases due to the lack of proper precautions.”[2]

Lost or compromised patient information can lead to financial identity theft, insurance fraud, or to medical identity theft that can plague victims’ medical and financial lives for years. It can result in erroneous entries in a person’s existing medical records or fictitious medical records in the victim’s name. As medical information is shared among hospitals, physicians and insurers, false information can propagate far and wide, leading to a host of problems, including the potential for life-threatening misdiagnoses.

Understanding the Growth of Cyber Threats

The threats associated with cyber attacks have grown significantly in recent years, as nearly all software, devices, and applications now connect to the Internet. Examples include billing systems using electronic transfers, medical devices uploading information real-time into patient electronic health records, and the increase in cloud-based file sharing. The risk grows when organizations consider the use of hospital-issued and personal laptops and mobile devices, and the availability of free Wi-Fi to patients and visitors. The web of data that is available continues to grow, as does the complexity of keeping it secure.

Attacks are Rapidly Increasing. According to the Ponemon Institute’s “Third Annual Benchmark Study on Patient Privacy & Data Security,” 94 percent of health care organizations have been victims of a cyber attack—94 percent of the surveyed organizations had at least one data breach in the past two years, and 45 percent had more than five incidents during that same time period. This is a drastic increase from 29 percent in 2010.[9]

A separate report released by Redspin in 2014 confirms the trend, reporting that nearly 30 million Americans had their personal health information breached or disclosed since 2009. The report identified 199 incidents of breaches of protected health information (PHI) in 2013, impacting over seven million patient records. That’s an increase of 138 percent in PHI breaches between 2012 and 2013.[7]

Cyber Threats Vary. One of the more commonly recognized threats are attempts to steal employee and patient data to sell in online black markets. While the reported payment per stolen medical record varies, a

(Continued on page 7)

PRESIDENT'S NOTEBOOK

Steven J. Summer
President and CEO

Dear Governing Board Members:

Although there is good reason for caution in today's wired world, there are plenty more reasons to feel optimistic about the opportunities technology presents for health care. As you read about cyber threats, miscommunications and security breaches, I hope you won't let it dissuade you from pioneering and adopting new technologies in your hospital. Colorado has made incredible technological advances that promise to improve care in every corner of our state.

There are two primary Health Information Exchanges (HIEs) operating in Colorado, the Colorado Regional Health Information Organization (CORHIO) and the Quality Health Network (QHN). CORHIO is the largest HIE and the officially designated HIE for the state with 31 hospitals, more than 1,300 office-based providers, 123 long-term and post-acute care facilities, 21 behavioral health centers and three large medical laboratories connected to its HIE. QHN, based in Grand Junction, has operated the longest and most of its providers are concentrated on the western slope with 12 hospitals and 19 other health care providers participating.

Why is this important? HIEs allow physicians and other qualified providers faster access to patient information. This saves time and money and often eliminates the need for duplicate tests. Electronic health records standardize information so that providers receive results in a consistent format and reduce the risk of errors and spending on unnecessary medications, tests and treatment.

I would be remiss if I didn't mention the incredible work the Colorado Telehealth Network (CTN) has accomplished. CTN currently provides subsidized broadband connectivity to 200 behavioral and physical health care sites in Colorado, allowing providers to establish a secure electronic connection with CORHIO and QHN. When it is fully deployed, CTN will link more than 400 hospitals, behavioral health providers, clinics and other health care groups throughout rural and urban areas of the state. CTN has also launched a statewide image exchange service, the Colorado Image Exchange, which allows for storage and retrieval of clinical and diagnostic images.

As your hospital engages in its strategic planning, I encourage you to view technology with your eyes wide open and from all perspectives. Yes, as with any new and somewhat untested frontiers, there are inevitable risks, but technological advances also promise to reduce health care costs, improve the efficiency and quality of care, provide needed specialist communication and allow for life-saving treatments. I believe that's worth exploring.

Sincerely,

Steven Summer, President and CEO
Colorado Hospital Association

Do you have ideas for future issues of *Colorado Trustee*?

Our goal is to provide you with the information and knowledge you need to lead your hospitals forward in today's rapidly changing environment. Tell us what you think, and what you'd like to see in future issues of *Colorado Trustee.*

Write or call:

Sandy Merrill 7335 East Orchard Road, Ste. 100 Greenwood Village, CO 80111 (720) 330-6024 sandy.merrill@cha.com

LEADERSHIP PERSPECTIVES

Communication Connection: Maximizing Relationships in a Technology-Centered World

New York Times bestselling author Joseph Grenny recently conducted an online survey in which 89 percent of those surveyed indicated that insensitive or inappropriate uses of technology - Electronic Displays of Insensitivity (EDI), were hurting their relationships by creating "digital divisiveness".[1] Others report that while technology can improve communication between physicians and patients, how it's used (for example, breaking eye contact, turning one's back to face a monitor or screen, or stopping to navigate the electronic health record or type notes) can create barriers to effective communication.

Whether its an everyday social interaction, patient-physician communication, or interaction between hospital leaders and board members, technology increasingly plays a role. Technology is an unparalleled tool for enhancing and strengthening communication, one that is rapidly changing our culture. Hospitals and health systems must be adept and innovative in leveraging the benefits technology offers across a variety of settings and for any number of purposes. But like many things, our greatest strengths and benefits can also be our Achilles heel. Technology can enhance communication, but it isn't always able to replace the connections essential to strong and effective governance leadership and can detract from or undermine relationships and leadership potential.

You Can't Always Just "Call In"

Today's health care environment with all its changes, challenges and complexity, requires boards of trustees who not only communicate, but who ensure they are engaging in the deeper dialogues that matter most. Governance conversations should be vibrant and vital, with trustees engaged in the verbal back and forth volley of constructive challenges to conventional thinking and the exploration of new alternatives. Through deep discussion, decisions are negotiated by wrestling with concepts, ideas and potential solutions. The creative energy that evolves during a hearty debate around the board table can't happen, or can't happen as easily, without the ability to read other trustees' non-verbal cues. We know the cues that signal a trustee's engagement vs. disinterest, buy-in vs. dissention, and misperception vs. understanding. These signals are essential to the effective communication necessary to conduct the critical work and leadership of the board.

The trick for trustees is discerning when face time should take precedence over technology and ensuring that technology remains a tool, not a default.

Attending every meeting in-person isn't always realistic. But many of the complex issues, negotiations and decisions that trustees must address require the clarity of communication that happens best with face to face interactions. It is the job of every trustee to consider the commitment he or she made to the hospital and its leadership, and determine whether that commitment can be fulfilled by calling in via telephone or video conference to a meeting, or if it requires in-person attendance. Busy schedules and long travel times may prevent this attendance at times, but if connecting to meetings remotely is a regular occurrence for some trustees, the board may need to re-evaluate its policies and practices for in-person meeting attendance.

When Presence Takes Precedence

A key concern with email, texting and tweeting, is the opportunity for misperception and miscommunication. At the board level, the stakes are too high to allow misinterpretations and misunderstandings to happen; however, despite the value of face-to-face interactions, time, distance, cost-savings and convenience make electronic communication an important and useful reality. The trick for trustees is discerning when face time should take precedence over technology and ensuring that technology remains a tool, not a default. Being present and taking part in face-to-face discussions may be most important in the situations outlined below.[3, 4]

Building new relationships and establishing trust. Strong working relationships and trust are especially important not only between trustees, but also with the CEO and members of the community. Being present provides opportunity to add depth to a relationship by putting names with faces, and adding knowledge of one another through the non-verbal communication that is exchanged.

Strengthening unity of purpose. Diverse opinions, ideas and perspectives among trustees is critical to avoiding "groupthink" and identifying new opportunities, but must be focused on moving the

(Continued on page 6)

GOVERNANCE INSIGHTS

Governing in a Wired World

Gone are the days when you go the hospital lab to get your blood drawn, and wait for a letter in the mail or a follow-up appointment with your physician. Today, you can complete a well check-up with a quick finger prick and receive a full print-out of your blood test results in minutes. Soon, this may be done at home using an iPhone. And that's just the tip of the iceberg. Medical technology is changing in ways that drastically alter the way health care is delivered, and ultimately the way patients utilize and perceive the health care system.

When led by boards encouraging ahead-of-the-curve thinking, hospitals have the potential to maximize technology in ways that improve patient care and patient quality of life, while at the same time maximizing efficiency in a budget-restrained world.

Despite this potential, health care organizations have lagged behind other industries in technology adoption for years. While health care information technology (IT) is making great strides, hospitals and health systems' electronic medical records lack standardization and generally are not yet integrated across care providers. In the last few years, "meaningful use" has become a well-used term in hospitals across the country as they strive to achieve the IT objectives encouraged by the Obama Administration.

Part of the lag in technology adoption is due to the need for a long-ingrained cultural shift in the industry, as health care advances in its transition from an environment of independent, solo practices and stand-alone hospitals to a large scale coordinated effort that relies on technology and care coordination.

In areas of both information technology and medical technology, health care providers have great opportunities ahead. While IT has been much-talked about, the field of medical technology and the growth of "mHealth" is just beginning to gain momentum. In some instances, the opportunities are unknown and introduce new risks. But in today's world, hospital leaders have a lot to gain by taking the plunge. Although Facebook can take risks that health care organizations must be cautious about taking, hospital leaders can still take note from the concepts the social media company uses with its employees—"done is better than perfect," and "the riskiest thing is to take no risks."

When it comes to patient care, quality is number one. But upgrading to the current socially accepted uses of technology and becoming a more efficient organization require improved utilization of technology, which may compel hospital leaders to cautiously try new approaches. In today's rapid-change health care environment, taking no risks can be quite risky.

mHealth: Changing the Way Health Care is Provided

Mobile health, or "mHealth," is more than the availability of health information online. mHealth is the wide variety of portable, mobile interfaces generated by smartphones, tablets and tablet PCs. It began as simply viewing health information and basic provider information with mobile devices. It has expanded to scheduling appointments online, emailing physicians and receiving emails or text messages with physician responses and appointment reminders, and providers' transition to using mobile devices in patient rooms rather than large computer stations. Now mHealth is evolving further, encompassing mobile health monitoring and diagnostic testing.

mHealth Has Great Potential, but Remains in Early Stages. Americans own more than 300 million mobile devices.[6] mHealth has the potential to improve patient experiences, minimize unnecessary care at a time when the health system is projected to be highly overloaded, and reduce costs. According to an American Hospital Association report, mobile health can reduce the need for hospital admissions and physician office visits. Survey results have reported that 40 percent of physicians said they could eliminate 11 to 30 percent of office visits through the use of mobile health technology such as remote monitoring, email or text messaging with patients.[1]

Mobile devices also have the potential to significantly strengthen home monitoring, further reducing office visits and preventing unnecessary hospital admissions or readmissions. Dr. Eric Topol, a cardiologist and one of the world's top physicians, has become a well-known expert in the growing field of wireless medicine and remote monitoring. He describes how the potential of the smart phone is being explored, including new ways it is just beginning to be used, and innovations that are not yet fully tested. Modifications and "apps" (applications) allow smartphones to conduct an echocardiogram, saliva test, sweat test, blood test, perform a portable ultrasound, and even monitor a patient's vital signs wirelessly.

In the U.S., home care accounts for about three percent of national health spending. Labor accounts for two-thirds of home care, and technology represents only a small fraction of costs. Increased technology use in home care has the potential to prevent or delay the shift of patients to acute care or long-term care settings.[1]

Apps are Growing, but Hospitals Face Challenges. Within physician offices and hospitals, mobile medical applications are growing profusely. New apps are continually being developed that share best practice standards and protocols, allow for "video conferencing" with remote translators or medical experts, and much more. Smartphones, iPads and tablet PCs are also increasingly used in place of "old-school" computer work stations. One study reported that these mobile devices are now used in 80 percent of health care organizations. At the same time, half of the survey respondents in a recent health care IT poll indicated that nothing is being done to protect data on devices that are often individual devices brought to the site—otherwise known as the "BYOD" (bring your own device) revolution.[1]

HIPAA and other regulations do pose greater challenges to the adoption of mobile technologies when compared to other industries. But as consumers' preferences and expectations for technology escalate, health care organizations must catch up to other industries in their use of mobile technology. John Reed, senior executive director of Robert Half Technology, reiterated this importance in a recent news release about health care organizations lagging in their use of mobile technology, stating that "Compliance issues have made it difficult for the health care industry to move as quickly as other sectors, but as consumer demand for mobile health information grows, formal mobile strategies are a necessary next step."[5]

E-Visits Can Improve Efficiency. The prevalence of "e-visits" is also growing, allowing patients and physicians to connect via texting and emailing. A recent study reported that the use of telephone and email visits cuts office visits by 26 percent,[1] a trend that has great potential to ease provider shortages and patient wait times in the coming years.

Technology Improves Patient Care

Improved quality of care is a critical component of health care reform. New technologies can improve care through a variety of ways, from clearer documentation to improved communication between providers to simply removing human error and interpretation from the patient care equation. As a result, hospitals will face continuing pressures to implement systems like computerized physician order entry (CPOE). Many hospital leaders believe that the increased use of technologies such as bar-coding of medications and drug-alert systems hold the most promise for reducing errors, a concept that is reinforced by the Institute of Medicine (IOM), which argues that the implementation of a bar coding system could reduce medication errors by 70 percent in some hospitals.

The quality of care in hospitals and outpatient care settings can also be maximized through data review and analytics. As electronic health records and CPOE systems are increasingly implemented and expanded upon, there is great potential for guidance and decision-making tools based on data history. While only a small percentage of hospitals implemented data analytics tools last year, more than half of hospitals are expected to do so by 2016. Data analytics can help identify patterns and insights that improve treatment and reduce costs.[4]

According to McKinsey & Co., "Big Data" could create $300 billion in value by reducing health care spending by eight percent. In 2012, health care generated an estimated 150 exabytes of health information. McKinsey & Co. believes that the massive data sets generated by health care activity could add value to health care by making information more transparent and quickly accessible, enabling better performance measurement through digital capture, and improving business analytics and decision support.[1]

New Technologies: A Sample of What's to Come

New technologies are emerging at a rapid pace. Some are available now, while others are still in the research and development phase. In the next decade technology has the potential to revolutionize the way health care is perceived and administered in the U.S. and around the world. A few examples of technologies available today and on the horizon in the near future include:[1,2,3]

- The ability to track every medication that is ingested, using pills tagged with digestible sensors activated by a change in the stomach pH
- Wireless sensors that monitor provider activities, such as nurse and physician hand washing
- An iPhone eardrum app that checks for an ear infection
- A modified iPhone that performs an electrocardiogram
- A non-invasive blood glucose monitor that wirelessly transmits blood sugar information to a smartphone or other wireless device
- A remote ICU monitor allowing patients to be monitored from home
- A portable ultrasound that transmits via a smartphone, allowing a real-time remote doctor visit and discussion of the results
- Nano sensors in the blood stream that pick up signals of precursors to a heart attack, and calls the patient's cell phone with a special ring tone warning that a potential heart attack is imminent
- A pill that can detect DNA fragments from cancer cells long before any tumor becomes visible
- Individualized medicine that is catered to each individual's health history and genetic make-up

Sources and More Information

1. American Hospital Association. 2013 Environmental Scan. www.aha.org.
2. Synderman, Nancy. iDoctor: Could a Smartphone Be the Future of Medicine? *Rock Center.* NBC News Video. January 24, 2013.
3. Weinstock, Matthew. Hospitals & Health Networks. Personal Interview. HealthForum-AHA leadership Summit, San Diego, CA. July 29, 2013.
4. Infographic: 5 Healthcare IT Trends Transforming Healthcare. *HIT Consultant.* April 10, 2013. www.hitconsultant.net.
5. Gregg, Helen. Report: Healthcare Lags Other Industries in Mobile Strategy. *Beckers Hospital Review.* March 26, 2014.
6. Gregg, Helen. 3 Challenges Faced by the mHealth Industry. *Beckers Hospital Review.* March 19, 2014.

(Continued from page 3)

organization in the same direction. For boards of trustees, that unity of purpose should be rallied behind fulfilling the hospital or health system's mission.

The stakes are high and decisions are critical; or when issues are complex and solutions are not readily apparent. Critical conversations and dialogue are the foundation for well-informed and innovative solutions. Without constructive challenges to conventional wisdom and give-and-take debate, the best solutions may never surface.

Issues are sensitive and the potential for conflict is high; or when conflict resolution is needed. When handled with respect and purposeful dialogue, short-term tension and disagreements can be constructive opportunities to building stronger understanding and appreciation for the disparate views among board members.

Seeking the engagement and views of others; or when seeking commitment, priority or sense of urgency from others. Miscommunication and misjudgment are often the result of inadequate listening, which can happen easily when separated by technology. To ensure strong, effective communication and connection, trustees should listen attentively without distraction or rushing to judgment to absorb information and acquire new ideas.

Persuasion and negotiation are required. The board's success is highly dependent on how trustees interact with each other, with the CEO and with members of the community. The ability to influence outcomes is highly dependent on the ability to connect personally with others, to understand their perspectives and to respond effectively.

Confidentiality is critical. Board members are in a position of trust, and in recognition of the sensitivity of the information entrusted to them, have a fiduciary responsibility to keep certain information secure and confidential.

Organizational performance is lagging and motivation, inspiration and leadership must be evident. Hospital boards must value creativity and innovation, and leverage change for strategic advantage. They must lead an organization that can capitalize on the new opportunities emerging from the rapid change occurring in health care today. Leadership that inspires and motivates others to succeed is driven by an authentic message that connects the organization in a personal way to a compelling vision and mission.

The issue, event, organization or purpose is important. Showing up and being present is a demonstration that a person or persons, event, organization or purpose is important to the trustee and worthy of investing personal time to support.

Ensuring Clear E-Communication

In her article, "Is Social Media Sabotaging Real Communication," Susan Tardanico offers tips for ensuring messages and issues are well-communicated.[2] Steps trustees should take to ensure their e-communication is not working against them include:

- Short-circuiting email exchanges that seem to lead to conflict by calling or talking in person;
- Double checking out-going communications for possible misinterpretation;
- Recognizing that different generations have different communication preferences—older generations typically prefer to speak over the phone or in person, while younger generations generally prefer text or email messages;
- Not hiding behind technology. Technology makes it easy to avoid difficult people, conflicts and other challenging situations, but true leadership requires engagement;
- Doing what you say, ensuring actions are consistent with written communications; and
- Circling back to make sure the message was received and correctly understood.

Technology Mishaps That Don't Occur When Face-to-Face

- The video connection is lost and must be re-connected
- The telephone is muted but the speaker doesn't know it
- The connection is so poor that the in-meeting participants cannot understand what the teleconferenced trustee is saying
- Telephone or web-conferenced trustees speak up but no one notices over the in-person meeting noise
- Last-minute materials are printed and not emailed to connecting participants
- The connected trustee simultaneously checks his or her email, makes a sandwich, or multi-tasks in some other way that detracts the meeting from their primary attention
- Breaks and meals facilitate relationships and side conversations, while remotely connected trustees remain isolated and separated from critical conversations

It's the job of the board to set the tone for the rest of the organization. Interacting with other board members in person helps foster not only a better knowledge and understanding of other trustees and their viewpoints, but can fuel a stronger unity of purpose and synergy among board members, and lay a foundation of trust within the board. By their presence and engagement, board members demonstrate the importance of the hospital's mission and its commitment to the organization and the community. Through its presence, the board has the opportunity to lead and inspire others.

Sources and More Information

1. Digital Divisiveness: Electronic Displays of Insensitivity Take Toll on Relationships. Crucial Conversations, VitalSmarts Research. www.vitalsmarts.com. Accessed March 18, 2014.
2. Tardanico, Susan. Is Social Media Sabotaging Real Communication? www.forbes.com. April 30, 2012.
3. Richman, Barbara. Face-to-Face Communication Can Help You Accomplish Business Objectives. www.bizjournals.com. August 17, 2013.
4. Grossman, David. Leading in Person: Six Reasons to Communicate Face-to-Face. The Grossman Group. www.yourthoughtpartner.com. August 31, 2011.
5. Tardanico, Susan. Five Habits of Highly Effective Communications. www.forbes.com. November 29, 2012.
6. Wilson, Jerry S. Don't Displace Face to Face. *Bloomberg Businessweek.* www.businessweek.com February 20, 2009.
7. Torrieri, Marisa. How Technology Interrupts Physician-Patient Communication. *Physicians Practice.* www.physcianspractice.com. November 20, 2013.

Health Care Providers Face Significant Risk

In February 2014, SANS, the largest source for information security training and security certification in the world, published a research study analyzing the impact of cyber attacks on organizations of all types. Data from the health care sector was analyzed from September 2012—October 2013. The report concluded that:[1]

- Health care's critical information assets are poorly protected and are often compromised.
- Providers of all types and sizes are at risk—no health care organization is immune.
- When organizations are compromised, they are often out of compliance for months or longer, meaning they aren't detecting their compromises or outbound malicious communications.
- During the study period, health care providers had the largest percentage of malicious web traffic emanating from them, accounting for 72 percent of all malicious traffic. Health care providers were followed by health care business associates (9.9 percent) and health plans (6.6 percent).

(Continued from page 1)

recent study reported that the cost to health care organizations is approximately $233 per stolen record, when accounting for incident handling, victim notification, credit monitoring, and projected lost opportunities.[1] Other attacks may be focused on gathering information about medical innovations or technologies, or may be more terrorist in nature, with the goal of harming patients by disabling devices or modifying medical devices.[3]

Unsecured Devices and Computers Contribute to Risk. According to the recent Ponemon Institute report, 81 percent of organizations allow employees and medical staff to use their own mobile devices to connect to their networks. At the same time, only 54 percent of the survey respondents reported confidence that the personally owned mobile devices are secure.[9] According to Redspin's President and CEO Daniel W. Berger, portable devices' lack of encryption is one of the greatest risks, stating "It's only going to get worse given the surge in the use of personally-owned mobile devices at work. We understand it can be painful to implement and enforce encryption but it's less painful than a large breach costing millions of dollars."[7]

In addition to unsecured mobile devices, hospitals continually use medical devices that contain sensitive patient information such as radiology imaging software or wireless heart pumps, 69 percent of which are not secure medical devices.[9]

Cloud computing is another risk, with nearly all organizations reporting that they use cloud services. At the same time, 47 percent are not confident that the information on the cloud is secure.[9]

The Financial Impact of Vulnerabilities

Privacy breaches can threaten the short and long term financial health of a hospital. The hospital board has responsibility for compliance, and the Health Information Technology for Economic and Clinical Health (HITECH) Act increased fines for non-compliance with HIPAA privacy regulations to $1.5 million per incident. New privacy and security requirements in the HITECH Act widen the definition of what health care information must be protected and make health care providers and their business associates mutually responsible for protection of shared patient data. The Act also sets specific thresholds, response timelines, and methods for breach victim notification, with potential fines for non-compliance ranging from $25,000 to as much as $1.5 million.

The Economic Impact Continues to Grow. Recent studies estimate that the economic impact of one or more data breaches for a health care organization ranges from less than $10,000 to more than $1 million. However, the average economic impact of a health care organization's data breach in the last two years is $2.4 million.[9]

The Greater Financial Risk May Be Loss of Patient Trust. While fines are significant, damage to the organization's reputation and loss of patient goodwill has the potential for much more devastating and long-term effects than any regulatory penalties. Even more than most business relationships, the provider-patient relationship is based on trust, and when any business loses a customer's personal data, the customer loses trust. A separate Ponemon Institute study found that lost business, not response costs, accounts for 65 percent of data breach costs.[5] Based on provider responses and customer loss figures from recent studies, Ponemon estimates that the average health care organization loses over $9 million every two years just to patient churn from data breach incidents, and that privacy-related breaches costs U.S. hospitals almost $6 billion a year. The potential loss may grow further if class-action lawsuits are incurred following a breach.

Board Responsibilities in Cybersecurity

While cybersecurity does not fall into the traditional realm of board roles and responsibilities delegated when hospital boards were first established, today it should be a critical component. Trustees

(Continued on page 8)

Examples of Recent Breaches

According to a recent report, protected health information (PHI) data breaches increased 138% in 2013.[7] Recent examples include:[6,7,8]

- Theft of four desktop computers from an office at Advocate Medical Group in 2013, which may have exposed more than four million records. Risks associated with unencrypted laptop thefts are growing as more mobile devices are utilized.
- An online security weakness at WellPoint, which serves nearly 36 million people through its affiliated health plans. Unauthorized users accessed personal data for 612,402 people between October 2009 and March 2010, ultimately resulting in a $1.7 million penalty to HHS for HIPAA violations.
- Hacker access to a server containing patient and employee records at St. Joseph Health System in Bryan, Texas in December 2013. While it remains unknown if or how the information will be misused, more than 400,000 people were compromised in the attack.

(Continued from page 7)

are responsible for protecting both the hospital and its patient community; and data breaches threaten both.

Elevate the Priority. While many health care leaders are aware of the risks, causes of, and ways to prevent data breaches, some continue to believe that prevention of patient data loss or theft is not a priority for their organization.[4] This is where trustee leadership is necessary to bridge the gap between knowing and doing. Security policies and budgets are a governance issue. And to govern effectively, boards need to stay abreast of current trends and methods for improving data security.

Eighty-one percent of organizations allow employees and medical staff to use their own mobile devices to connect to their networks. At the same time, only 54 percent report confidence that the mobile devices are secure.[9]

According to the recent Ponemon study, the most common causes of data loss or theft were unintentional actions by employees, including lost or stolen computing devices, followed by employee mistakes or unintentional actions. And while the growth in electronic health records (EHR) brings significant potential for improved patient safety and coordination of care, the reality is that electronic records create a new set of security concerns. Digitized records make patient data available to more people inside and outside the hospitals, leaving it vulnerable to hackers and cyber-thieves.

Ensure the Board's Role in Oversight. The American Hospital Association (AHA) recommends that hospital boards assign cybersecurity to a relevant board committee to provide more detailed oversight and governance. The hospital's ongoing cybersecurity investigations and plans should be reviewed with the committee, and, if an intrusion does occur, either the full board or the committee should be briefed on the event, lessons learned, and modifications to the hospital's security plans as a result. The AHA also recommends that the board's audit committee provide oversight into cybersecurity vulnerabilities and potential exposures, including insurance coverage.[3]

Set Security Goals. The board or the appropriately assigned board committee should set privacy and security goals for the hospital. Goal setting should begin with an assessment of current security measure and risks. An expert, objective third-party assessment can measure the hospital's exposure to data breach and whether existing security measures are sufficient. For example, many organizations do not know where all their patient information was physically located or where the greatest vulnerabilities lie. An initial assessment provides a benchmark for setting goals and measuring the success of subsequent security measures.

Staff for Security. Day-to-day security within the hospital environment depends on effective oversight and effective security processes. Security programs are likely to be more effective if someone in the organization "owns" data security and privacy – usually a chief security officer, chief privacy officer, or compliance officer. If no such position exists, trustees can help assess and determine what kind of staffing will best fit with the organizational structure. Once an owner is in place, the board should support that person with adequate staffing and funding for personnel-related initiatives such as security screening and on-going training in security procedures, in addition to needed system and process improvements.

AHA: Six Actions to Manage Cybersecurity Risks

The American Hospital Association recommends the following six actions to manage hospital cybersecurity risks:[3]

1. Establish procedures and a core cybersecurity team to identify and mitigate risks, including board involvement as appropriate.
2. Develop a cybersecurity investigation and incident response plan that is mindful of the Cybersecurity Framework being drafted by the National Institute of Standards and Technology.
3. Investigate the medical devices used by the hospital in accordance with the June 2013 FDA guidance to ensure that the devices include intrusion detection and prevention assistance and are not currently infected with malware.
4. Review, test, evaluate, and modify, as appropriate, the hospital's incident response plans and data breach plans to ensure that the plans remain as current as possible in the changing cyber threat environment.
5. Consider engaging in regional or national information-sharing organizations to learn more about the cybersecurity risks faced by hospitals.
6. Review the hospital's insurance coverage to determine whether the current coverage is adequate and appropriate given cybersecurity risks.

Sources and More Information

1. Filkins, Barbara. Health Care Cyberthreat Report. A SANS Analyst Whitepaper. February 2014.
2. Comey, James B. Director, Federal Bureau of Investigation. Statement Before the House Appropriations Committee, Subcommittee on Commerce, Justice, Science, and Related Agencies. Washington, D.C. March 26, 2014.
3. Cybersecurity and Hospitals. American Hospital Association. 2013.
4. Ponemon Institute. Benchmark Study on Patient Privacy and Data Security. November 2010.
5. Ponemon Institute. 2007 Annual Study: U.S. Cost of Data Breach. November 2007.
6. Landen, Rachel and Conn, Joseph. WellPoint to Pay $1.7 Million HIPAA Penalty. *Modern Healthcare.* July 11, 2013.
7. Sacramento Press Releases: Redspin Reports on the "State of Healthcare IT Security." *PR Newswire.* February 5, 2014.
8. Gregg, Helen. Data Breach at St. Joseph Health System Affects 400K. *Becker's Hospital Review.* February 6, 2014.
9. Ponemon Institute. Third Annual Benchmark Study on Patient Privacy & Data Security. December 2012.