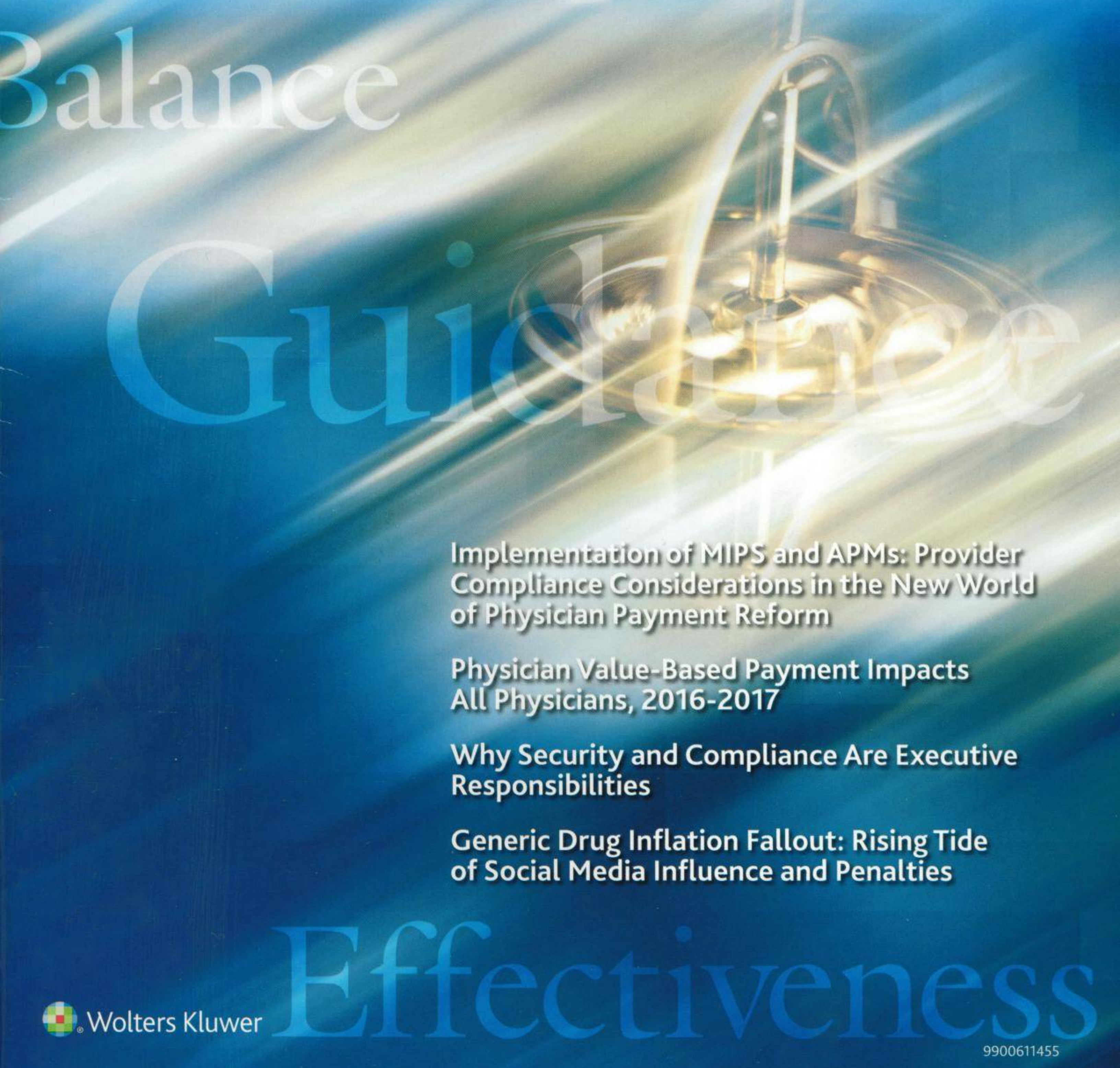
March–April 2016

Journal of Health Care Compliance



Implementation of MIPS and APMs: Provider Compliance Considerations in the New World of Physician Payment Reform

Physician Value-Based Payment Impacts All Physicians, 2016-2017

Why Security and Compliance Are Executive Responsibilities

Generic Drug Inflation Fallout: Rising Tide of Social Media Influence and Penalties

Wolters Kluwer

9900611455

Why Security and Compliance Are Executive Responsibilities

Preventing Executive-Level Embarrassment and Career Damage

Mike Semel

Mike Semel is the president and chief compliance officer for Semel Consulting. He can be reached at 888/997-3635 ext 101 or by email at mike@semelconsulting.com.

Your executive team can deal with security and compliance now, and invest adequate attention and resources, or they can deal with it later trying to explain to an angry public why you had a data breach or an information technology (IT) security crisis.

Security and compliance are executive-level challenges that need top-level support and adequate financial resources, yet many executives prefer to delegate these responsibilities to lower-level managers and staff. They often cut budgets and ignore risk warnings because they do not think anything will ever happen. They think that security and compliance are tactical issues, not strategic problems that could kill your organization. They do not understand what their lives will be like if a security or compliance crisis occurs.

Ask your top executives, "If we suffer an IT security failure or data breach, who in our organization do you think will be dealing with the media, our board of directors, our clients/patients, investors, lawyers, and our insurance companies?"

In the November – December 2015 issue of *The Journal of Health Care Compliance*, Art Weiss, chief compliance and ethics officer for TAMKO Building Products, recommended showing your executives the recent Department of Justice (DOJ) Yates memo suggesting that the DOJ will be prosecuting more people in leadership roles. For many reasons it is much better for the executive team to prevent a crisis rather than try to explain it to stakeholders. Public opinion is everything. They need to get involved.

Hospital Data Held for Ransom

There are a lot of lessons to be learned from the recent ransomware attack on a California hospital that caused them to transfer patients and be the subject of national media attention. From Healthcare-infosecurity.com:

> …no organization is immune to outbreaks of **malware** that's designed to forcibly encrypt all data stored on PCs and servers. Hollywood Presbyterian Medical Center, based in Los Angeles, declared an "internal emergency" after staff noticed an apparent **ransomware** outbreak begin on Feb. 5, reports NBC. The attackers have demanded 9,000 bitcoins, currently worth about $3.6 million, reports Fox News.
>
> The hospital couldn't immediately be reached for comment. But as of Feb. 12, multiple patients had been transferred to other hospitals as a result of the attack, electronic patient records remained inaccessible, and all hospital departments — lacking email access — were attempting to communicate via "jammed fax lines," NBC reports.

In an open letter, Allen Stefanek, Hollywood Presbyterian Medical Center President and chief executive offier (CEO) said the hospital paid $ 17,000 to gain access to its data. The letter said the news reports that the ransom was $ 3.6 million were incorrect. (How many more people saw the news articles compared to the PR letter on the hospital's Web site?)

The letter says "this incident did not affect the delivery and quality of the excellent patient care you expect and receive from Hollywood Presbyterian Medical Center ("HPMC"). Patient care has not been compromised in any way."

The crisis ended on February 15, *10 days* after the attack, after transferring patients, and after national embarrassment. After transferring patients and being forced to communicate via "jammed fax lines," does anyone really believe that the incident did not affect their "excellent patient care?" How did not having access to medical records, or medical devices controlled by computers, affect patients? How many will sue for malpractice? Will any die?

Naturally, everyone wants to know what the cause was, but that will have to wait for later. Based on almost every other major data breach and hacker attack, the root cause was probably an employee simply clicking on a link in a phishing email.

Whose heads do you think will roll, after the investigation that will probably show that *this attack could have been prevented or resolved with little impact*? Every executive in every type of business needs to selfishly think, *"How would an attack like this affect my career, my family, and my future?"*

This type of crisis can be avoided. Recently a doctor in a medical practice clicked on a link in a phishing email, and a few minutes later the practice received a ransom note that all of its data had been encrypted. Instead of paying the ransom (which doesn't always get your data back) they called their IT provider who was able to recover their data from the previous hour's backup and get them working again. They had to re-enter a few medical notes, but otherwise they were unaffected.

There are lessons to be learned from every breach. The Sony and Target attacks were both based on phishing emails. In the Target breach the hackers accessed the network by compromising an air conditioning vendor, not the company itself. Neither CEO survived the fallout of these attacks.

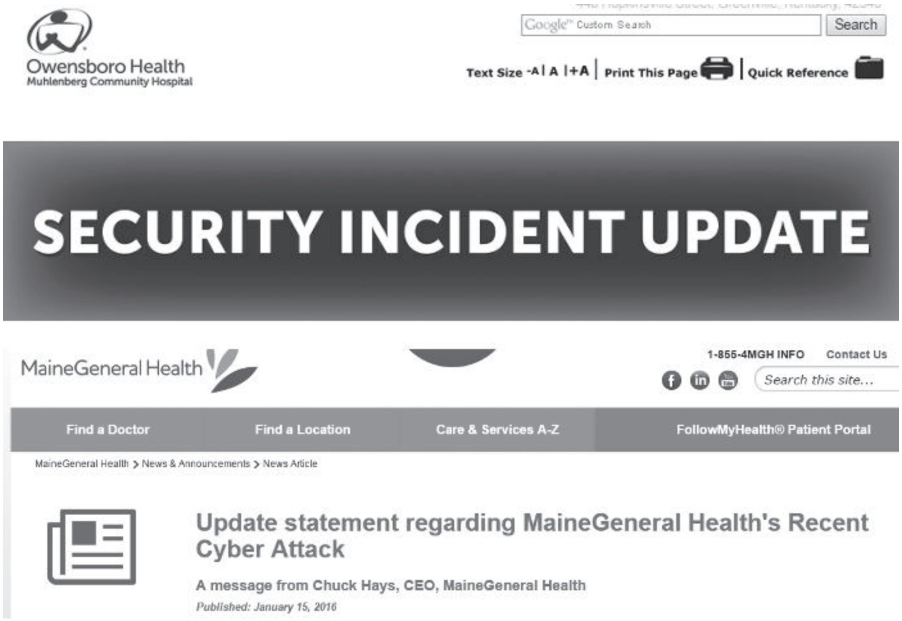
Ask your executives if they want the Web site you use to build trust and generate business to look like one of those in Figure 1.

Here are some things your organization can do right now to prevent an expensive and embarrassing situation.

Get a Second Opinion

Engage an outside consulting organization to evaluate your security, and compliance with regulations, and make sure the report goes directly to your CEO, managing partner, or the board of directors. Our assessments always find holes — sometimes very large ones — in IT security because most

Figure 1:



SECURITY INCIDENT UPDATE

Update statement regarding MaineGeneral Health's Recent Cyber Attack

A message from Chuck Hays, CEO, MaineGeneral Health

Published: January 15, 2016

IT departments (and outsourced IT service providers) are made up of good desktop computer and network specialists, but not IT security specialists. There is a big difference.

The FBI alerted health care organizations in 2014 that the greatest risk to the security of their data was the belief their IT departments had that their efforts were working, *when the evidence showed otherwise*.

This was substantiated in late 2015 when two hospitals — one in Kentucky and the other in Maine — were notified by the FBI that their data was for sale on the Internet. Forensic examinations showed that one was breached in 2012 and the other in 2013, meaning that for 2 to 3 years the hackers were in the hospital's computer systems without being detected.

When someone in your organization says they "have security and compliance handled," it is time for an outside expert's opinion. Your executives need an "under the skin" evaluation of your security and advice from an experienced compliance expert who can explain the findings in business terms they understand, not IT jargon.

Know Where Your Data Is

This sounds simple, but many organizations we work with start out not even being able to identify all the locations of their data. Data is a valuable asset, like gold, but is often treated casually, and no one cares until it is lost, stolen, or held for ransom. Why is valuable and protected data left on unsecured local PCs and laptops? Why isn't it backed up in case of accidental loss or hard drive failure? Why is it allowed to be shared through unsecure consumer-grade cloud services? Knowing the locations of your data is even more critical if your data is protected by laws like the Health Insurance Portability and Accountability Act (HIPAA).

Know Your Backups Really Will Work When You Need Them

Backups are no good if they do not protect your data *and* if they cannot be restored both within your required timeframe and with minimum data loss. Backups need to be test-restored regularly to ensure that your *functions* can be restored, not just some data or a server.

We still see organizations that back up to tape, local hard drives, or even consumer-grade cloud services. These are inexpensive solutions that can take days to restore and sometimes fail completely.

What is your real cost of being down? Hollywood Presbyterian Medical Center has already lost revenue and will have to spend a lot to secure its network and recover its reputation. A law firm managing partner once estimated their cost of downtime at $ 64,000 per day and was shocked when their IT director confirmed our estimate that their backup strategy would keep them down for three to four days. A medical practice whose backups we discovered were not going offsite told us they would have to go out of business if their building burned down and they lost all their patients' records.

Once your executives figure out your real cost of downtime, they will realize it is worth the investment for secure backups that run throughout the day and allow you to recover servers quickly (usually less than an hour) to a local recovery appliance, or to the cloud if your building burns down. What may seem like high monthly fees will pay off when you can quickly recover and avoid the high costs and embarrassing publicity of a disaster.

Fund the Security You Really Need

Security is more than anti-virus software and firewalls (which we often find are not properly configured). Funding an effective security program is critical to your mission.

Security starts with how your network shares are configured and who has access to critical, sensitive, or regulated data. It is amazing when we see critical and sensitive data on network shares set to be accessed by "everyone." We also find that terminated employees still have access to the company networks, and their passwords are set to never expire.

You need systems that log your network activity *and* detect unauthorized access. More than anything, you need to employ or contract with IT security specialists (not your average IT specialists) who can properly configure secure tools and address any incidents.

Do Not Ignore Your Vendors, Even Those You Like and Trust

While organizations focus on their internal compliance programs, they often ignore their vendors. Under HIPAA and other regulations, if one of your vendors causes a breach, then you are required to notify your patients, and you can be liable for fines. The HIPAA Omnibus Final Rule (2013) dramatically increased the requirements and liability for business associates (vendors), although many think they do not have to do anything else once they sign a business associate agreement. The new HIPAA audit program will include business associates if a covered entity receives an audit letter.

Executives need to be firm with vendors, including long-trusted law firms and accountants, who ignore compliance requirements. They must be willing to end relationships if the vendor might cause a compliance violation or breach through its ignorance or inadequate compliance efforts.

We recently worked with a health care client to survey its vendors about their HIPAA compliance. The law firm that is currently defending the client in a medical malpractice case denied that it had to do anything special to comply with HIPAA "because they had to implement security measures to protect client data related to real estate transactions."

While there are common themes to secure data of all types, HIPAA has some specific requirements that are not met by complying with a different regulatory standard. For example, did the law firm sign a subcontractor business associate agreement with the expert witnesses they hired to review medical records to support their client's defense?

The compliance officer passed her information to her managers. The executives now have to accept the risks related to the attitude of their lawyers, or push them to revisit HIPAA.

Data Security Is More Than Technology. Train Your Staff!

The weakest links in any secure environment are people, who are the last line of defense against an attack. Even with the best IT security systems in place, users need to be trained and reminded against falling for the lure of phishing emails that bait them into clicking on dangerous links. They need to be wary of official-sounding phone calls asking for their logins and passwords. They need to know it is okay — actually required — to stop strangers in restricted areas to ask who they are.

Training is critical for all staff, not just new employees. It should not be a meaningless 5-minute 2-slide presentation just to get a requirement out of the way. The C-level executives should authorize the time to make sure your staff receives effective cybersecurity and compliance training, including those in the executive suite where the bosses sometimes think they are too important or too busy. Management should set an example, partly because executives have been identified as carelessly clicking on links in phishing email tests.

Research into data breaches shows that most of the financial impact is in reputation damage and lost business. Regulatory fines can exceed a million dollars. Executives can lose their jobs.

Remember, security and compliance are strategic … not tactical.

A list of related articles can be found at www.semelconsulting.com/blog.

Reprinted from Journal of Health Care Compliance, Volume 18, Number 2, March–April 2016,
pages 17–21, with permission from CCH and Wolters Kluwer.
For permission to reprint, e-mail permissions@cch.com.