SAME-DAY SURGERY

THE TRUSTED SOURCE FOR HOSPITALS, SURGERY CENTERS, AND OFFICES FOR MORE THAN THREE DECADES

MAY 2017

Vol. 41, No. 5; pp. 49-60

INSIDE

Tips for preventing cyberattacks 51

Avoid common mistakes writing plans of correction 52

Here are some survey do's and don'ts . . . 54

Joint Commission issues Sentinel Event Alert about leadership's role and safety culture. 54

Recognizing signs of workplace intimidation 56

SDS Manager: Reader Feedback, Part Two 57

Smart strategies for containing OR costs 58

AHC Media
A RELIAS LEARNING COMPANY

Cyber Criminals Increase Damaging Attacks Against Healthcare Organizations

'Ransomware' is latest threat

Healthcare providers are cyber criminals' low-hanging fruit. Patient records are valuable on the black market of the dark web. So are employment records and the latest scourge: ransomware.

Ambulatory surgery centers (ASCs) and any healthcare organization that relies on electronic data could be attacked. Any ASC that is subject to federal privacy regulations also is at risk for regulatory problems related to a security breach.

"Anybody that is a covered entity under HIPAA is at risk," says **Dan L. Dodson**, president of Fortified Health Security in Franklin, TN.

"If your ASC has a breach impacting more than 500 medical records, you have to report it, and you can have big problems if there is no risk management program," Dodson says.

Cyberattacks are going to be one of the biggest issues healthcare organizations face going forward, Dodson says.

"As there's more publicity around this, it will drive more people to focus on healthcare," he notes.

> "AS THERE'S MORE PUBLICITY AROUND THIS, IT WILL DRIVE MORE PEOPLE TO FOCUS ON HEALTHCARE."

Experian's 2017 Data Breach Industry Forecast says that healthcare organizations continue to be the most targeted sector for hackers. Problem areas include medical identity theft, stolen medical information, and ransomware.

Financial Disclosure: Editor **Jonathan Springston**, Editor **Jill Drachenberg**, Author **Melinda Young**, Nurse Planner **Kay Ball**, RN, PhD, CNOR, FAAN, Physician Editor **Steven A. Gunderson**, DO, and Consulting Editor **Mark Mayo** report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study. **Stephen W. Earnhart** discloses that he is a stockholder and on the board for One Medical Passport.

SAME-DAY
SURGERY

Same-Day Surgery®,
ISSN 0190-5066, is published monthly by AHC Media, a Relias Learning company,
111 Corning Road, Suite 250, Cary, NC 27518

Periodicals Postage Paid at Atlanta, GA 30304 and at additional mailing offices
GST Registration Number: R128870672

POSTMASTER: Send address changes to:
SAME-DAY SURGERY
P.O. Box 74008694
Chicago, IL 60674-8694

SUBSCRIBER INFORMATION:
Customer Service: (800) 688-2421
Customer.Service@AHCMedia.com
AHCMedia.com

SUBSCRIPTION PRICES:
U.S.A., Print: 1 year (12 issues) with free *AMA Category 1 Credits*™ or Nursing Contact Hours, $519. Add $19.99 for shipping & handling. Online only, single user: 1 year with free *AMA Category 1 Credits*™ or Nursing Contact Hours, $469. Outside U.S., add $30 per year, total prepaid in U.S. funds.

MULTIPLE COPIES: Discounts are available for group subscriptions, multiple copies, site-licenses, or electronic distribution. For pricing information, please contact our Group Account Managers at Groups@AHCMedia.com or (866) 213-0844. Missing issues will be fulfilled by customer service free of charge when contacted within one month of the missing issue date. Back issues, when available, are $83 each. (GST registration number R128870672.)

ACCREDITATION: Relias Learning, LLC is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation.

This activity has been approved for 1.75 nursing contact hours using a 60-minute contact hour.

Provider approved by the California Board of Registered Nursing, Provider #CEP13791, for 1.75 Contact Hours.

AHC Media, LLC is accredited by the Accreditation Council for Continuing Medical Education to provide continuing medical education for physicians.

AHC Media, LLC designates this enduring material for a maximum of 1.75 *AMA PRA Category 1 Credits*™. Physicians should claim only the credit commensurate with the extent of their participation in the activity.

This activity is intended for outpatient surgeons, surgery center managers, and other clinicians. It is in effect for 24 months after the date of publication.

Opinions expressed are not necessarily those of this publication. Mention of products or services does not constitute endorsement. Clinical, legal, tax, and other comments are offered for general guidance only; professional counsel should be sought for specific situations.

AUTHOR: Melinda Young
EDITOR: Jonathan Springston
EDITOR: Jill Drachenberg
AHC MEDIA EDITORIAL GROUP MANAGER: Terrey L. Hatcher
SENIOR ACCREDITATIONS OFFICER: Lee Landenberger

PHOTOCOPYING: No part of this newsletter may be reproduced in any form or incorporated into any information retrieval system without the written permission of the copyright owner. For reprint permission, please contact AHC Media, LLC. P.O. Box 74008694
Chicago, IL 60674-8694. Call: (800) 688-2421.
Web: AHCMedia.com.

"Ransomware is when they lock down your system and get you to pay ransom in response," says **F. Paul Greene**, Esq., chair of the privacy and data security practice group at Harter Secrest & Emery in Rochester, NY.

Cyber Trends Change

A few years ago, cyberattackers focused on collecting credit card information. But the payment card industry tightened their controls, so cyber criminals shifted to collecting healthcare records, Greene explains.

"To make a comparison, on the dark web, a credit card number can go for pennies — less than a dollar," he says. "A healthcare record sells for tens of dollars. The last statistic I've seen is that one [medical] record could cost $40 on the dark web."

One appeal of healthcare records is that they often include Social Security numbers as a common identifier. "Many of our usernames had the last four digits of our Social Security number, and any part of your Social Security number can be dangerous if it's leaked out there," Greene says. "It can lead back to who you are and result in identity theft."

Medical records contain a wealth of information for criminals. They can use records to open bank accounts, apply for credit cards, and to fraudulently bill Medicare and Medicaid, Dodson says.

Ransomware is one of the newer and more pernicious forms of attack. Typically, when someone in a surgery center or hospital opens an innocuous email and clicks a link, that opens the computer to an infection. The ransomware bug is designed to encrypt an electronic system's data so that no one can view the information without a key. The attackers offer to sell the key to the victim for thousands of dollars. Many healthcare organizations will pay the fee because they can't function without their data for long.

Organizations that lack a sufficient data back-up and recovery plan may not be able to restore systems quickly, and they have no choice but to pay the ransomware price, Dodson says.

"I also believe that when some folks are paying the ransoms, it will lead to more bad behavior," he adds.

"You'd be surprised at the very sophisticated individuals who fall into a ransomware scheme," Greene says. "They can pay bad guys to use their ransomware service and send out infected links to collect the ransom."

The infected emails appear to be from a trusted source, and they're typically well-written. The age of the Nigerian prince emails with multiple grammatical errors are over, he notes.

EXECUTIVE SUMMARY

Cyber criminals, seeking access to medical records or to lock files until receiving a ransom, continue attacking healthcare providers.

- Any ambulatory surgery center that uses electronic data is at risk.
- Common problems related to breaches are medical identity theft, stolen medical information, and ransomware.
- Organizations that pay the ransom compound the problem, encouraging more attacks.

For instance, an attacker might discover through social media that someone attended a particular university. Then, the attacker will send an email that appears to originate from that university's alumni association, asking the person to "click here" for reunion registration information, Greene explains.

"The reason why ransomware has exploded in healthcare is that healthcare really depends on immediate access to its electronic systems," he says. "There has been a big push for electronic medical records."

When a surgery center's or hospital's electronic systems are down, the healthcare organization is under tremendous pressure to fix the problem; therefore, they will pay the ransom, just as Hollywood Presbyterian Hospital did in 2016. The hospital paid $17,000 in ransomware, a drop in the bucket when faced without full access to its electronic system for 10 days, Greene says.

"They could not perform certain procedures or certain tests because their system was down," he adds. "That's catastrophic for a healthcare provider."

The typical ransomware price is around $3,000. Attackers often ask that it is paid in bitcoin, an online currency with a fluctuating cost of around several hundred dollars per bitcoin.

"It's a smash-and-grab kind of thing, and we expect to keep seeing this kind of attack for the foreseeable future," Greene says.

"Under HIPAA, ransomware now is a reportable breach, and healthcare providers must conduct a four-factor risk analysis to decide whether they should let HHS know," Greene says. "And HIPAA is not the only story. When they have a ransomware attack, they also have to look at other federal and state laws that might apply."

Ransomware and other breaches are legal issues, as well as security issues. Nearly all states have instituted breach notification rules. From an ASC's perspective, this could mean learning the breach notification rules of many states. Every patient the ASC has seen has a record in the electronic file, and these patients could be from different places.

"That's the new frontier for healthcare providers, and many are not aware or prepared to deal with the regulatory complexity," Greene says. "How do relevant laws apply, and how do you meet those standards?"

HIPAA's recent guidance outlines ransomware specifically because some experts claimed it wasn't a breach since the attackers do not take information away from the healthcare facility, Greene notes.

"HHS said that even if they don't get the information, ransomware is a potential reportable breach and subject to a four-factor breach analysis under HIPAA," he adds.

From a security perspective, ransomware circumvents technical controls because someone has unknowingly opened the system's door and let the bad guy in, Greene says. "You can have a wonderful firewall and security system, but that action by a user will circumvent all of those users."

As soon as the security industry develops a strategy for addressing the attacks, the criminals — who often are from foreign countries with no extradition policy with the United States — will find a way to circumvent the security solution.

"Ransomware is easier than stealing data, and the answer is that the hackers are opportunistic, creative, and lazy — they go for the path of least resistance," Greene says. "Why hack into Microsoft when you can send out 1,000 ransomware attacks and get $3,000 or $4,000 each time it works?" ■

Tips to Prevent Cyberattacks

Cybercrime prevention requires a plan for how to back up data, assess a system for vulnerabilities, manage cybersecurity, and handle regulatory and legal repercussions should a breach occur.

"Take a proactive approach. Monitor logs, look at vulnerabilities, and watch for trends over time," suggests **Dan L. Dodson**, president of Fortified Health Security.

"First, you need an understanding of potential vulnerabilities within your environment and the potential exploitability of those," Dodson explains.

For instance, an ASC might use old technology that prevents it from deploying a security patch, he says. "You have to plan around how to navigate that risk, and one way is by monitoring it."

Cybersecurity monitoring can detect actions that indicate someone is trying to breach the system. Monitors would note that at midnight, someone tried to change the admin login or enter an admin password dozens of times.

"That's not normal, and if one of

our analysts picked up on that, we would call the client and say, 'Did you get a new admin and upgrade the system last night?'" he says.

Without monitoring the system for breaches, an organization might never know about a security problem.

Another tactic is to invest in adequate backup for the computer system and files. This should be part of a HIPAA risk assessment, says **F. Paul Greene**, Esq., chair of the privacy and data security practice group at Harter Secrest & Emery.

"This should be part of your HIPAA risk assessment — to look at data and the systems and assess how often it has to be backed up," Greene says.

If a surgery center saves its data every day, then a breach or ransomware attack would result in a limited amount of data loss.

Finally, if a site has been the victim of a ransomware attack, keep in mind that the attack is just the beginning of the problem, Greene says.

"You must have policies and procedures in place to comply with HIPAA obligations and state laws, and everything down to the local level. New York City has data security laws on the books," he explains. "It's an incredible patchwork you have to navigate when you have a breach."

Besides the legal issues that arise with a ransomware attack, there also is the additional cyber risk. Once a healthcare organization becomes the victim of a successful attack and pays the ransom, they're going to be attacked again. Plus, the decryption key does not work instantly. It can take days to regain access to data after paying the ransom and obtaining the key, Greene warns.

Healthcare organizations that lack an adequate risk management plan for cyber threats could be vulnerable if a breach occurs and the facility is investigated by the Office of Civil Rights, Dodson notes.

"The way they run their assessments is they don't hold a small [ASC] to the same standards as a hospital," he explains. "They'll compare the reasonableness of its plan to its peer group. But the answer cannot be, 'We have not done an assessment.'"

One of the biggest challenges an ASC might experience in addressing cyber threats involves educating staff about cybersecurity and how they can prevent threats, Dodson says.

"The best advice I can give people is it is top-down. Everybody, from the CEO to management, has to be aware of this and focused on educating their employees," he says.

There is affordable technology that can fake a phishing campaign and highlight which departments and/or staff need additional education, Dodson says. "Really being proactive is the best defense for that." ■

ASCs Can Avoid Common Mistakes When Writing Plans of Correction

If an ASC that treats Medicare patients has not been surveyed since 2015, it's likely time to expect one. In recent years, state health departments — fueled by federal funding — have increased survey inspections.

Since 2009, there has been increased government funding to assess ASCs' compliance with Medicare and other regulations. Most surgery centers will undergo a survey every three years, says **Jan Allison**, RN, CHSP, senior director of regulatory at AmSurg in Nashville, TN.

"Since 2009, the majority has been seeing a much larger increase in the volume of surveys taking place and the frequency with which they're happening," Allison says. "I worked for an [ASC] for 21 years, and state surveyors showed up twice during that time."

That was before 2009 when the regulations changed. CMS began paying more attention to ASCs in 2008 after a Las Vegas ASC exposed patients to hepatitis C. Additional ASCs were found to be in violation of infection control regulations.[1]

In early 2008, Nevada public health officials identified a hepatitis C cluster — the largest recorded — among patients of an ASC in Las Vegas. In all, they found nine linked and 106 possibly linked HCV cases among patients who underwent surgery on the same day as HCV-infected patients believed to be the infection's source.[2]

A Nevada state health division investigation determined that inappropriate syringe use caused the HCV cluster. Thus, Nevada increased its number of surveyors by one-third.[1]

State resources vary, so ASCs in some states will conduct fewer surveys. Also, there is the unpredictability of what will happen in the federal budget process this year. The president's budget, if enacted along with plans to reduce regulations, could result in scaled-back surveys.

Each state can be different in its

survey direction and focus, notes Allison, who assists AmSurg's surgery centers in 38 states with their plans of correction (POCs). *(See story on surveyors' pet peeves, page 54.)*

"In the past, surveyors were not as well trained as they are today in the level of detail and how they conduct surveys," she says.

Following a survey, ASCs must respond to the findings, and they do this through the POC. CMS and state agencies use the POC to verify deficiencies have been corrected, and the plan of correction is a legal document that is accessible to the public. Therefore, it's very important to write the POC well and accurately, Allison urges.

"If you look at the surveyor's deficiency report, it's very, very detailed," she explains. "People tend sometimes not to provide enough detail in the [POC], when they need to respond with the same level of detail as the report provided."

The short list of what to do to improve a plan of correction includes: "Identify and meet your deadlines. Identify staff responsible for oversight. Provide specific details. Have a monitoring plan," Allison explains.

The following are additional suggestions for improving the POC:

1. Read the cover letter thoroughly.

The cover letter explains precisely what state surveyors want in the POC.

"Some states want the [POC] put into the report you received, and some might provide you with a form of their own," Allison says.

The cover letter includes the findings in an attached 2567 report describing whether any deficiencies were found and, if any were found, describing those deficiencies.

Other information to glean from the cover letter includes:

• Where and how do you submit the POC?

• By what date do corrections need to be completed?

• Who do you contact with questions?

2. Know the hot topics in deficiency reports.

While infection control issues are always big on surveyors' lists, in recent years, the deficiencies have focused increasingly around environmental/life safety issues, Allison notes.

"It's about the environment — that's where more than half of the deficiencies are coming from," she says. "If something hasn't been done, then you get a contractor out there and make sure it's done and not missed, going forward."

Humidity monitoring was a chief focus two years ago. Now, the focus is on air flow, Allison says.

"Does an area require a positive or negative air flow environment, and is that being maintained?" she says. "Other problems we've seen in the last few years are related to life safety."

Life safety surveyors will assess:

• if the ASC is maintaining its generator appropriately;

• if the facility has completed and documented all fire alarm system inspections and maintenance;

• if smoke detectors have undergone required sensitivity tests.

3. Demonstrate how the ASC will measure success.

"Monitor to show your strategies are working," Allison says. "Describe how you did something to improve compliance. That tells the surveyor you took this seriously and did something a step above and beyond just saying you will do a better job."

For example, if a deficiency is noted in hand hygiene, it's not sufficient to say, "We held an in-service on hand hygiene." A better strategy is to meet with staff to solicit their input as to why they were not compliant, Allison says.

It could be the hand cleaning product causes skin to be dry and irritated. If this is a problem, then part of the solution would be to switch products. Other solutions would be to post hand hygiene posters at each sink and provide ongoing education and training, including instruction on use of specific products. Also, an ASC could reinforce good hand hygiene behavior through positive, ongoing feedback, she suggests. ■

EXECUTIVE SUMMARY

ASCs have been subjected to frequent regulatory surveys since a Las Vegas ASC was linked in 2008 to a cluster of hepatitis C cases.

• It's important for ASCs to create a well-written, well-detailed plan of correction (POC) in response to survey results.

• The POC verifies that deficiencies have been corrected.

• Read the surveyor's cover letter carefully and follow those instructions when writing the POC.

REFERENCES

1. Harasimlas P. Deficiencies found at Nevada ambulatory surgical centers. *Las Vegas Review-Journal*, March 9, 2009. Available at: http://bit.ly/2n0oGuZ. Accessed March 27, 2017.
2. Mathis S. Closing in on health care–associated infections in the ambulatory surgical center. *J Leg Med* 2012;33:493-528.

Some Survey Do's and Don'ts

Most important: Sign the report

ASCs easily can avoid some of the more common problems encountered when writing a POC in response to citations.

A simple solution is to sign the report, says **Jan Allison**, RN, CHSP, senior director of regulatory at AmSurg.

The bottom of the report might list "laboratory director" or some other title, but that's because the same survey reports are used for various healthcare facilities. Just sign the report and date it, Allison says.

The following are some other do's and don'ts:

• **Give separate answers for each item in one system citation.** The survey citation will list findings, but some of these will not be one-off problems. They'll be related to a system issue, and this should be explained, including why it happened, Allison says.

"A facility could receive a sanitary environment citation based on surveyors finding dust, not cleaning beds according to manufacturer's instructions, and not maintaining an autoclave," she says. "When someone writes the correction, write a separate correction for each of those observations, if they're different."

• **Note who is responsible for inspections, but don't use actual names.** "You don't put in people's names, only their titles," Allison says. "It's the same for listing vendors."

If an ASC has contracted with a fire alarm vendor, don't include that company's name in the POC, she advises.

"The [POC] is public information," she explains. "Anyone can request a copy from the state for review, or, in some cases, find it on the internet via a search engine."

Plus, surveyors don't want to know the name — they just want to know the role and title, Allison adds.

• **Ensure leadership is involved.** ASC leaders ultimately are responsible for every correction and monitoring results. Each finding during internal monitoring should be reported to a committee, such as a quality committee, as well as to leadership, Allison says.

• **Watch deadlines.** "Make sure deadlines listed on [the] POC are not too soon and can't be met," Allison says. "Don't say, 'I can have that done next week,' because what if there is a snowstorm and the ASC didn't get to have the in-service?"

Instead, provide a realistic deadline with a built-in time cushion that still meets the deadline established by the state.

• **Include attachments, if surveyor wants them.** Submitting attachments with a POC can be supportive evidence. For instance, if an in-service already was conducted on a citation issue, then the sign-in form with the in-service topic could be attached. Likewise, an organization could attach an invoice showing that a problem area was repaired, Allison suggests.

Just remember that some states do not want an attachment; the cover letter will provide that information.

"Most states are fine with that," she says. "But others say, 'Take that reference out of there.'"

• **Be prepared for detailed questions.** Some surveyors will dig into the details. For example, a surveyor might note that a firewall has an unsealed penetration hole in it. The hole might have been the result of installation of cables. Provide details in the POC to indicate what kind of product was used to caulk the hole, Allison says.

"Was it a commercial, fire-rated substance?" she says. "Keep it simple, but still provide details like these in the [POC]." ■

Joint Commission Issues Sentinel Event Alert About Leadership's Role and Safety Culture

Healthcare, including ASCs, leadership plays a role in driving a safety culture, according to The Joint Commission.

"Leaders in all organizations that deliver care have to be responsible for building a culture of safety," says **Ana Pujols McKee**, MD, executive vice president and chief medical officer at The Joint Commission in Oakbrook Terrace, IL.

"You cannot make improvements in healthcare without a solid foundation of a safety culture," McKee says. "Whether its surgical site infections, wrong surgery, falls — whatever problems, if you have not built a safety culture, then you will not be successful in reducing or eliminating harm."

The March 1 Sentinel Event Alert states that The Joint Commission has found that inadequate leadership can contribute to adverse events, including the following issues:

- offering insufficient support of patient safety event reporting;

- lacking feedback or response to staff and others who report safety vulnerabilities;

- allowing intimidation of staff who report events;

- refusing to consistently prioritize and implement safety recommendations;

- failing to address staff burnout.[1]

McKee makes the following suggestions for improving an organization's safety culture:

• **Review the organization's core values.** "The first thing a leader does is go through the core values or code of conduct or description of safety culture," McKee says. "They have to articulate that clearly and make sure everyone in the organization knows what those values are."

Leaders also must demonstrate these values through their actions and address any poor behaviors in their staff.

• **Encourage open communication.** "One principle of safety culture is to allow people to speak up freely," McKee says. "That means behaviors that intimidate or ignore quiet people have to be eliminated."

Daily, leaders should exhibit open communication and crack down on intimidation.

"It's not something you do once a week," McKee says. "Every day, the leader has to demonstrate and lead by example."

The way a leader does this is by letting nurses, surgeons, and others know that behavior that intimidates staff is not acceptable. The goal is to create a culture where people are comfortable, she explains.

• **Prevent and stop intimidation.** Intimidation by supervisors or workplace authorities can destroy open communication. It can create an unsafe atmosphere by making employees feel that if they speak up about a problem or unsafe situation, they will be ignored or worse.

"Intimidation can be subtle or very apparent," McKee says. "It could be rolling your eyes when someone is asking a question, or not answering a pager or someone's question."

Intimidation includes body language or words that suggest, "That's a stupid question" or "Isn't that something you should know?"

The danger of intimidation shuts down lines of communication. Supervisors need feedback from staff to learn about obstacles to safety and quality care. "The price of shutting down someone is huge," McKee says. "We know through a Sentinel Event database that it's not rare to hear of someone in a surgical arena who knew it was the wrong surgery, but the safety culture was missing, so the person didn't speak up."

Although it may seem difficult to imagine an employee not speaking up when there's something unsafe or wrong with a surgery, it happens, she notes.

"It could be the wrong surgery, wrong person, wrong procedure, wrong site — any of those," McKee says. "The reality is that a person who has been chronically intimidated behaves differently than someone who has been respected."

Leaders can stop unintentional intimidation by pointing out these disrespectful behaviors to the people involved. If the intimidation is intentional, then leaders should have a conversation explaining that the behavior is unacceptable in this organization, and if the leader sees it happen again, he or she will take disciplinary action, McKee says. *(See story on signs of staff intimidation, page 56.)*

"You have to be very firm around someone who is trying to dismiss or intimidate another staff member," she says. "Say it's inconsistent with the organization's values, and the organization will not tolerate those behaviors."

• **Assess system strengths and vulnerabilities.** Organizations should proactively assess medication management, electronic health records, and other system strengths and vulnerabilities.

For instance, with medication management, a surgery center could assess high-risk medications by performing a failure mode and effectiveness analysis, McKee says.

With each high-risk medication, ASC leaders could identify potential problems and rank the three most likely possibilities. Then, they can put in place a mitigation plan, she explains.

"You put into your process defense mechanisms or protections in the areas where you think there is the most risk," she says.

An example might be the risk that a medication is administered to the

EXECUTIVE SUMMARY

Surgery center leadership plays a crucial role in creating an organizational safety culture, according to a recent Joint Commission Sentinel Event Alert.

- Leaders should follow and review the organization's core values.
- Leaders must encourage open communication among staff.
- Leaders must eliminate and prevent intimidation in the workplace.

wrong patient. The prevention plan would create a policy requiring two clinicians at the bedside whenever the medication is administered. One clinician would check the medication and dose.

"Build in redundancy in how it's administered," McKee says. "And you do that for every possible risk that you have identified as having a likelihood to happen."[1]

• **Develop a baseline measure of safety culture performance.** The Joint Commission recommends that organizations use a tool developed by the Agency for Healthcare Research and Quality called the Hospital Survey on Patient Safety Culture (HSOPS) or another tool, the Safety Attitudes Questionnaire.

The HSOPS identifies the following 12 dimensions of safety culture:

- communication openness;
- feedback and communication about error;
- frequency of events reported;
- handoff and transitions;
- management support for patient safety;
- nonpunitive response to error;
- organizational learning;
- overall perceptions of safety;
- staffing;
- supervisor/manager expectations and actions promoting safety.[1]

Although these are hospital tools, McKee recommends ASCs use them.

"There may be questions not relevant to that clinical environment, but when it comes to behavior, communication, and professionalism, it's applicable across the healthcare spectrum," McKee says. "It demonstrates their commitment and understanding of their safety data."

• **Consider accreditation.** Although non-hospital-based ASCs are less likely to see accreditation, it's something they should consider, McKee suggests.

"For a freestanding center, it's not necessarily something they would do, but this is very important for them to take on in the future," she says. "Their issues are equivalent to other settings in the hospital."

Accreditation could be one of the most important actions an ASC could take to improve its clinical environment, she adds.

"It's a way to standardize their processes and give them a platform to improve," McKee says. "Since so much has shifted to the ambulatory side, it's in the public's best interest for ambulatory surgery centers to be accredited." ■

Recognizing Signs of Workplace Intimidation

Workplace intimidation is similar to domestic intimidation. Both make people behave in ways that are hard to explain and justify, says **Ana Pujols McKee**, MD, executive vice president and chief medical officer at The Joint Commission.

"When you silence someone, all of these things go through their minds: 'Am I right? What if I'm wrong?'" McKee says. "We want to eliminate that in healthcare because we want everyone to voice their concern."

McKee offers the following examples of workplace intimidation:

• **There are fewer event reports.** A workplace in which employees are intimidated tend to report events reported to the organization less frequently, she says.

"If a person feels that putting in a report about something that is unsafe can cause the person punitive consequences, then the person doesn't make the report," McKee explains.

• **Employees are fired for process failures.** When a workplace's culture includes staff intimidation, scapegoats are blamed for problems that are systemic.

"You might find that people have been fired for things related to process failures and not people failures," McKee says.

• **New ideas are stifled.** If employees never or rarely offer new ideas to improve the organization, it could be because they are afraid to be innovative, McKee says.

"Their new ideas are not rewarded," she says.

• **Leaders are unaware of the negative culture.** Sometimes, an organization's leadership is unable to appreciate that the culture does not promote safety. For instance, the leadership might wrongly celebrate few safety problem reports, not realizing the lower number is because of employee intimidation, McKee says.

"They don't appreciate that numerous reports are a sign of a healthy culture," she adds. "So bad behaviors are tolerated, and employees feel they cannot speak up because leadership does not support a safety culture." ■

REFERENCE

1. The Joint Commission. Sentinel Event Alert 57: The essential role of leadership in developing a safety culture. Available at: http://bit.ly/2lqJbge. Accessed March 27, 2017.

Reader Feedback — Part Two

By Stephen W. Earnhart, MS
CEO
Earnhart & Associates
Austin, TX

As promised in the April issue, here is the second part of my column about reader feedback to the March article, "Things I Notice."

I have replied to all who emailed me, so if I missed you and didn't get your message, please send again. In all, there have been more than 100 emails and 375 comments. I appreciate all the feedback.

11. Requiring patients to come to your facility two hours before surgery is ridiculous and just highlights your inefficiency. This hit a nerve with many people. Several responders offered excuses for why patients must be in the facility two or more hours before surgery and were "offended" that I would label this inefficient.

This is a service industry we all work in, which means we provide a service to our customers. I'll use Starbucks as another example of a service industry. Imagine that every time you went in for a cup, they told you that you must wait while they clean the machines and brew the coffee. You would say, "Why don't you do that before I come in?"

Many of you said you must allow for patients getting lost or showing up late or missing insurance papers, etc. However, those are excuses, not reasons.

Most people agreed that most of the time that is not the case. So, why are patients who comply punished for the actions of the minority? If a patient arrives late, then there should be better communications from staff.

If your surgeon wants to "stack" patients for high-volume cases, such as cataracts, gastrointestinal, or pain management cases, then you must increase your timing and communications for patients to make sure the surgeon has his or her next patient ready.

Bottom line: If it takes longer than 45 minutes to process a patient through registration and into the operating room, you are inefficient and must conduct a step-by-step review of why you cannot handle your patients in a respectful-of-their-time manner. Take the time to learn your bottlenecks and fix them.

12. Only 30% of facilities have instituted updated policies and procedures because the odds are you will get away with it. Sadly, there were only a couple of comments on this observation. There always is something more important to be done. Often, time doesn't allow for this function, which we all need to do. So, here is my best response when I am sitting with the medical director of a facility or the administrator of a facility that is out of date on their P&Ps: "Pretend that I am sitting in the jury box, and you are going to explain to me why you didn't have the time to update your procedures for the safety of your patients." It is effective.

13. Eighty percent do not capture all patient charges. I received more than 40 responses to this statement. Almost all agreed that many charges escape staff and cost the facility money. Review your process and hold a staff meeting to find a better way of capturing this money left on the table.

14. Ninety percent don't even know it. Most of the commenters didn't understand how they would know. Perform an "operational and process audit" on yourself. Ask a staff member or hire an outside company to conduct it for you. Audit your cases and make a note of everything used during those patient encounters. Compare the audit with what your staff submitted. Most of you will find a large discrepancy.

15. Most medical directors of ASCs have no idea what is required of them. Guess who sent me the most emails? Medical directors. There were a few management staffers who responded for their medical directors, which should tell you something. Most will be surprised to know that Medicare requires that the medical director has a job description and a contract that spells out exactly what is expected of them.

16. Elimination of the Affordable Care Act will have virtually no effect on your job. Not a single response.

17. About 99% of facilities are not equipped with enough supply or equipment storage space. This problem results in cluttered hallways and sterile corridors that make facilities look "trashy" to patients wheeled into the operating or recovery room. Almost everyone who responded agreed with this statement and wish they had more equipment storage space.

18. Most surgeons don't care about your personal issues. Save them for Facebook. I guess I must have been wrong about this, based on comments like, "My surgeons do care about my boyfriend issues," "Our docs want to see pictures of my child's birthday party," "I think it is important to share political feelings with the surgeons — they always seem interested in my opinions," "I can share my feelings with the surgeons that I cannot with my wife," and "I think it is important that the surgeons understand that if my child support payments were on time then I could fix my car and not be late so often." Interesting, but compare these responses with the next observation.

19. All staff resent surgeons talking about their new homes, cars, or boats while they struggle with day care costs and day-to-day expenses. A good surgeon is a quiet surgeon. That last sentence upset some surgeons; however, I received more than 100 emails supporting this observation from staff.

Earnhart & Associates is a consulting firm specializing in all aspects of outpatient surgery development and management. Earnhart & Associates can be reached at 5114 Balcones Woods Drive, Suite 307-203, Austin, TX 78759. Phone: (512) 297-7575. Fax: (512) 233-2979. Email: searnhart@earnhart.com. Web: www.earnhart.com. ■

Smart Strategies for Containing OR Costs

The first step to containing operating room costs is simple: Make cost containment a top priority.

"Make it something the entire facility wants to attain," says **Jennifer Butterfield**, RN, CNOR, CASC, administrator at Lakes Surgery Center in West Bloomfield, MI.

Butterfield offers the following tips on how ASCs can make cost containment a top priority:

1. Make everyone accountable.

Cost containment goals can be built into employees' performance improvement goals, annual merit pay, and bonuses, Butterfield says.

"Make sure employees don't spend if they don't have to, avoiding costs and reducing costs," she says.

"We have benchmarks in place so the cost containment and eliminating expense reduction initiatives are part of their annual merit and bonus pay," she says. "Each individual person has a few goals in their department that are aligned with cost containment."

2. Know your expenses.

"The two highest costs are staffing and supplies," Butterfield says. "For staffing, we pick productivity initiatives, and there might be 50 initiatives for which to set goals for staff."

For example, an initiative involving payroll would be to ensure everyone is punching in on time and not rounding up, she notes.

Or there might be an initiative to create a morning huddle. People can plan their day, and the leadership team can make sure each case is staffed adequately and efficiently, she says.

Another staffing strategy is to stagger start times. If there are late cases, then an ASC can bring in some staff at 9 a.m., instead of 7 a.m. This will prevent overtime pay when employees have to stay until 5 p.m., she suggests.

3. Make staff aware of costs.

"Staff has to be aware of costs, and having a culture of being aware of costs is important," Butterfield says. "One way to avoid cost is to have knowledge."

For example, if a sales rep meets with staff to sell a name-brand stainless steel pin for orthopedic and other surgical procedures, the staff should know the cost is almost three times the off-brand version that the facility has stocked, she explains.

"The job of the OR staff in the room is to keep costs in check by saying, 'We're not opening your product. We have our own,'" Butterfield says.

The same is true for surgeons. "Surgeons focus on patients; the sales rep's job is to talk the physician into that special magic wand," she says. "They see what the physician is struggling with, and their job is to say, 'I have this item that would be perfect for you to use where you're struggling.'"

When that happens, a nurse or tech in the operating room should be empowered to say, "We're not going to use that special magic wand because this one we're using works just as well," Butterfield says.

One way to empower staff to speak out is to teach them how to do so. For instance, they could ask sales reps how much the item costs.

"That puts sales reps on the spot," she says. "And then, they can say, 'Did the materials manager approve that?'"

It's not that an ASC cannot use the latest and greatest product, but sales reps should at least be made aware that there isn't an open checkbook when they visit the facility, Butterfield says.

4. Include physicians in purchasing decisions.

Most ASCs have group purchasing organizations (GPOs) that help reduce the cost of standard products, but their cost containment is less effective with the more expensive items, such as implants, Butterfield notes.

"The way to avoid high costs in implants is to develop a program where you get physicians together to talk about what types of implants they want to use and the type of volume they think they'll have," she suggests. "Then you can develop a contract with the vendor of that implant."

The decision could include a physician, administrator, and a materials/business office manager.

The key is to know the ASC's volume and types of surgeries. And ASCs should negotiate with different vendors. It can be cheaper to negotiate a price with one vendor than to use multiple vendors in buying similar items, she adds.

5. Hire a materials manager.

"There's a huge cost savings in having a materials manager," Butterfield says. "They can pay for themselves, and their only job is to manage all the products that come into the facility."

Small surgery centers sometimes make the mistake of placing a nurse or scrub tech in charge of ordering products, wearing a different hat after 1:30 p.m., she says.

"But those people are basically paying retail for products because they're not sophisticated enough in purchasing to make sure they have contracts," she adds. "It's not their full-time job to look at materials, look at shipping to make sure you're not spending extra for overnight shipping."

Without a materials manager, an ASC could end up with too much inventory on the shelves. Also, surgeons are more susceptible to sales pitches without a gatekeeper.

"The materials manager is the gatekeeper to having that vendor come in and say the doctor said we're going to use this product today," Butterfield explains. "The materials manager can say, 'I know the doctor said that, but you have to go through me, and we need to do a pre-cost verification."

6. Predict case-by-case costs.

The materials manager, the revenue cycle coordinator, and the administrator complete a form with cost and reimbursement information about a case. Based on the CPT code, the patient's insurance, and the requested items to be used in the case, the materials manager estimates the cost of the case, Butterfield says.

Then, the materials manager hands the estimate to the administrator, who determines whether the ASC can afford to take the case, she adds.

"A lot of times, I'll say, 'Go see if you can do it with a different implant,'" she says. "We know there are certain payers who don't pay well on certain things, and we're not here to take cases that don't make any money."

Not every case is red-flagged for scrutiny.

"We look at specific procedures that we know were based on historical data that you have to watch the margin on, and orthopedics is one because the implants are expensive," Butterfield says. "We also look at procedures where there are multiple things happening that might require [costly] disposables."

7. Regularly review custom packs.

Specialty packs should be reviewed every six months or once a year because habits change over time, Butterfield suggests.

"Make sure staff is not wasting items in the specialty pack," she says. "Make sure what we're putting in those packs is being used and not put aside. We tell staff to put anything they don't use in the pack into a box."

Regularly, someone checks the box to see what hasn't been used, and then these items can be taken out of the packs, she adds.

"A while ago, we found out that we were not using these towels," Butterfield explains. "On the very first case, they do a five-minute scrub, but after that they use an alcohol-based product for their second scrub of the day, so they only need the towel for the first scrub of the day."

A cost-effective solution was to take towels out of the packs and make towels available separately, so they could be pulled out only when they were going to be used.

That saved six cents per pack on 6,000 cases a year, she notes.

8. Use trial periods with new products.

Surgeons' gowns are important for comfort and other reasons, including movability, heat, and whether the gown withstands water.

When a surgery center wants to change to a new product for cost-cutting reasons, they can give the gowns or other product to staff to try and ask for their feedback, Butterfield says.

"We let them know there will be a three-week trial period, and then we get their feedback on whether they liked the gown or experienced breakthrough or felt overly warm."

9. Ask management for productivity initiative advice.

"Management has to pick different productivity initiatives," Butterfield says. "Make sure each department picks out an initiative from time clocks to a huddle to staggering start times to cross-training. They need to pick a few, master those, and then take another." ■

SAME-DAY SURGERY

CME/CE INSTRUCTIONS

To earn credit for this activity, please follow these instructions:

1. Read and study the activity, using the provided references for further research.

2. Log on to AHCMedia.com then select My Account to take a post-test. *First-time users must register on the site.*

3. Pass the online tests with a score of 100%; you will be allowed to answer the questions as many times as needed to achieve a score of 100%.

4. After completing the test, a credit letter will be emailed to you instantly.

5. Twice yearly after the test, your browser will be directed to an activity evaluation form, which must be completed to receive your credit letter.

CME/CE QUESTIONS

1. **What is ransomware, and why should a surgery center be concerned about it?**

   a. Ransomware is when burglars break into a surgery center, steal high-priced equipment, and hold it for ransom.
   b. Ransomware is when cyber criminals breach a surgery center's database and encrypt patient files until the site pays a ransom for the key to unlock the data.
   c. Ransomware is the name of the newest internet virus.
   d. All of the above

2. **When preparing a plan of correction after receiving a regulatory surveyor's 2567 report, which information in the report's cover letter could be useful?**

   a. Where and how you submit the plan of correction
   b. By what date must one complete corrections
   c. A person to contact with questions
   d. All of the above

3. **A March 1 Sentinel Event Alert states that The Joint Commission has found inadequate leadership can contribute to adverse events, including all of the following *except*:**

   a. offering insufficient support of patient safety event reporting.
   b. paying staff different salaries based on performance and experience.
   c. lacking feedback or response to staff and others who report safety vulnerabilities.
   d. allowing intimidation of staff who report events.

4. **What are the two biggest costs for ASCs?**

   a. Staffing and supplies
   b. Equipment maintenance and staffing
   c. Supplies and janitorial services
   d. Staffing and regulatory compliance