SAME-DAY SURGERY

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

OCTOBER 2015 Vol. 39, No. 10; pp. 97-108

INSIDE

AHC Media

ASC worker, about to be fired, moves patient files to personal email

What can you do to prevent a similar incident at your organization?

By *Joy Daughtery Dickinson*

An employee figured out that she was about to be fired by her surgery center. She responded by sending about 170 emails from her work computer to her personal email account. Those emails included personal information for 317 patients, including some highly sensitive files for in vitro fertilization patients.

"If you get mad when you get fired, you can't bust up the equipment. You can't steal a generator from the warehouse. You can't take money out of the register. You can't bust out the window on the way out," said **Robert R. Short II**, chief assistant district attorney, Office of the District Attorney, Wichita, KS, when talking to the jury. "All those things would be considered a crime. So what makes [an employee] think she can go in and data mine all this information and put it in her personal email?"[1]

"SOME EMPLOYEES CAN MOVE FROM TRUSTED TEAM MEMBER TO DISGRUNTLED EX-EMPLOYEE FAIRLY QUICKLY."
— MARK FULFORD, LBMC INFORMATION SECURITY

The surgery center discovered the emails had been transferred when they conducted an audit after she was fired, according to media reports.[1] The surgery center sent a letter to all of the patients affected by the email release.[1]

State law in that location prohibits employees from abusing their authority and taking confidential information from their employers' computers, Short said in an interview with *Same-Day Surgery*. He said this

Financial Disclosure: Executive Editor Joy Dickinson and Nurse Planner Kay Ball report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study. Mark Mayo, Consulting Editor, reports that he is executive director of Golf Surgical Center and executive director and a retained consultant of the ASC Association of Illinois. Physician Reviewer Kirby Scott, DO, discloses that he is consultant, stockholder, and on the speakers bureau for Entellus Medical. Columnist 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, LLC, One Atlanta Plaza, 950 East Paces Ferry Road NE, Suite 2850, Atlanta, GA 30326.

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 550669
Atlanta, GA 30355.

SUBSCRIBER INFORMATION:
Customer Service: (800) 688-2421.
customerservice@AHCMedia.com.
www.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, call Tria Kreutzer toll-free at (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.)
Missing issues will be fulfilled by customer service free of charge when contacted within one month of the missing issue's date.

ACCREDITATION: AHC Media, 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 1.37 nursing contact hours using a 60-minute contact hour.

Provider approved by the California Board of Registered Nursing, Provider #CEP14749, for 1.37 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.

EXECUTIVE EDITOR: Joy Daughtery Dickinson (404) 262-5410 (joy.dickinson@AHCMedia.com).
DIRECTOR OF CONTINUING EDUCATION AND EDITORIAL: Lee Landenberger.

EDITORIAL QUESTIONS
Questions or comments?
Call **Joy Daughtery Dickinson**
(404) 262-5410

type of law is relatively new.

The employee testified that she worked from home sometimes and that she had previously sent emails to her personal account. She also said that some of those previous emails had included confidential patient information. The employee testified that she feared repercussions from the surgery center about an incident of fraudulent insurance billing. She said her name was attached to the work, and she needed to be able to prove it was valid. The worker said she forwarded the emails to protect herself and that she had permission to send the emails.[1]

Her lawyer claimed that the emails were forwarded, rather than downloaded or printed, in order to be open and transparent. Her lawyer quoted excerpts from the employee handbook and said that only 4.2% of the emails sent contained patient health information. [1]

Seven emails had attachments with confidential patient information, and those emails were the primary focus of the case against the employee. A reproductive endocrinologist at the center said that the in vitro fertilization records were highly sensitive because patients often don't share such private information even with their family and friends, and it's "a very emotionally sensitive area of medicine."[1]

The jury found the employee guilty on all seven counts of computer fraud. At press time, she was scheduled to be sentenced Sept. 23.

5 steps to take

What can you do at your facility to avoid such an incident? Sources interviewed by *SDS* suggest the following:

• Educate employees on their security responsibilities.

"Some employees can move from trusted team member to disgruntled ex-employee fairly quickly," says **Mark Fulford**, CISA, CISSP, ABCP, partner at LBMC Information Security, an accounting and professional services firm with headquarters in Brentwood, TN.

Outpatient surgery managers must clearly communicate security responsibilities to employees, Fulford says. Before employees are given access to your IT systems, and preferably at least annually, go over acceptable access and use of data, he

EXECUTIVE SUMMARY

A surgery center employee who was about to be fired sent about 170 emails from her work computer to her personal email. Those emails included some highly sensitive files for in vitro fertilization patients.

- Before employees are given access to your IT systems, and preferably at least annually, go over acceptable access and use of data. Ensure your policies say that transferring electronic protected health data outside of the organization's network should be done only if specifically authorized.
- When firing employees, disable the access credentials, obtain any keys or equipment, and escort them while they obtain their belongings and leave the building.
- Examine new technology that can prevent electronic information from being transferred or downloaded.

says. "Reminding them of potential sanctions, which should be part of your written policies and procedures, is just as important," he says. Include training in HIPAA federal regulations regarding privacy and protection of patient information, experts emphasize.

• Carefully handle employees who are to be terminated.

When firing an employee is necessary or imminent, monitor and restrict the employee's ability to cause damage to your organization through removing assets, including health information, Fulford says.

"In the case of a 'hostile' termination, the employee's access credentials should be disabled, any keys or equipment obtained, and the person should be escorted while they obtain their belongings and leave the building," he says. "This sounds harsh, but it has become the world we live in."

• Examine use of protective technology.

Begin to evaluate Data Leak Prevention, or DLP, systems to protect your electronic patient health information, Fulford advises. "Technologies that can prohibit health data from being downloaded to removable media or transferred out via email are becoming more commonplace and will soon be seen as the standard of care for protecting against these types of insider threats," he says.

His views on using technology are echoed by **Marc Voses**, Esq., partner and co-chair of the Data Privacy Liability and Technology Services Practice Group, Kaufman Dolowich & Voluck in New York City. "The lessons from this case are that no matter what your employment policies are concerning the maintenance of confidential client information, unless you employ active electronic security measures that prevent the unauthorized emailing of information outside of the business' servers, you are at risk that confidential information can be accessed by an unauthorized individual either intentionally or negligently," Voses says.

He says "active electronic security measures" refers to computer software programs that allow office administrators to prevent information from leaving secured servers unless the employee has the appropriate credentials. "However, permitting an employee to move confidential patient information, or any proprietary business information for that matter, to servers that are not under the control of the business is unacceptable in this day and age due to the risk of unauthorized disclosure," Voses says.

Certain programs can be customized so that, for example, information can't be copied to portable storage devices, or it is automatically encrypted so that the information can't be accessed without a password, he says.

In the case mentioned earlier, the center was located in a state in which it was unlawful for employees to go beyond the authority they have to access and remove information from a computer. However, the deterrent effect of criminal laws is not enough to stop employees from improperly accessing or downloading confidential patient information, Voses says.

• Ensure your policies and procedures address the issue.

Have clear policies in place to prohibit removal of patient data, including physical records or electronic records, for anything except an approved business purpose, Fulford says. "There should also be evidence that employees have read and agreed to these policies as a condition of employment," he says.

Fulford says policies should spell it out: Transferring electronic protected health data outside of the organization's network should be done only if specifically authorized. "When authorized, there should be several controls considered in the policy," he says. Fulford says those controls should include the following:

— Encrypt data before it is sent.

— If sending to a third party, put appropriate business associate agreements in place before any data transfers occur.

— Maintain a list of parties, internal and external, that receive data transfers along with the nature, purpose, and frequency of the transfers, along with who authorized the transfers.

• Address work-at-home arrangements.

Fulford acknowledges that most organizations have remote workers. "However, there are ways to greatly reduce or eliminate the need for a home-based or remote worker to have electronic records stored or processed on their home computers," he says.

Provide access to clinical and billing systems through remote technologies, Fulford suggests. *(See Resources at end of this article.)* These technologies "leverage Internet technology such that an employee's home computer is actually displaying a computing session on a remote machine with the appropriate security controls," Fulford says.

Put controls in place that restrict the ability of the remote worker to store or print records to their local home office, he advises. "As a general security precaution, health records should not be stored on personal computers that are not maintained in a secure fashion by the facilities' IT or security teams," Fulford says. "Since home computers are often shared by

multiple family members and lack the perimeter firewalls and security controls that are in place at most facilities, the chance for compromise of those machines, and hence potential undetected data breaches of ePHI [electronic protected health information] is high." *(For information on how to protect yourself from a breach, see story in this issue.)*

REFERENCE

1. Dunn G. Former surgery center employee found guilty of computer crime. *Wichita Eagle*. July 20, 2015. Accessed at http://bit.ly/1JdMG2U.

RESOURCES

- **Citrix** in Santa Clara, CA. Telephone: (800) 424-8749 or (408) 790 8000. Web: http://bit.ly/1PwCpyF.
- **Remote Desktop Services** from Microsoft, Redmond, WA. Telephone: (866) 425-4709. Web: http://bit.ly/1KKmDN0. ■

Good computer logs critical to detecting breach

A detailed record of who accessed data, when, and how often might be the only way an organization can trace the source of a HIPAA breach. Ensuring the thoroughness of those logs should be a top priority for any healthcare organization, says former federal prosecutor **Thomas G.A. Brown**, senior managing director of the Global Risk & Investigations Practice with FTI Consulting in Washington, DC.

"Companies often do not have adequate logs, and so they don't even know what they lost or how it happened," Brown says. "They might know they've been breached, but they can't figure out what data was accessed, much less who is responsible."

It is a mistake to focus only on defending the computer system from attack, from outside or within, Brown says. Criminals eventually will find a way around even the best security, and recent incidents in which healthcare employees took screen shots show that insiders can steal data without leaving an obvious trail. But the computer log should reveal all, he says.

Internal segmentation of the data system should slow thieves, which prevents easy access across databases, but employees always will have access to protected health information (PHI), so Brown says the computer log can be used to determine when and how an employee accessed that data.

"The key thing is figure out what you lost, which is really important in the healthcare field, because you need to provide adequate notice to victims and other obligations under HIPAA," Brown says. "If you know you lost something, but you don't know what you lost, that's going to complicate your efforts to comply with HIPAA's obligations once you're aware of the breach." ■

FDA issues guidance on duodenoscope reprocessing

In the news: Another outbreak and warning letters to scope manufacturers

(Editor's note: We tweeted about this news on Aug. 5. To access breaking news as it happens, follow us on Twitter @SameDaySurgery.)

The Food and Drug Administration (FDA) has released guidance on supplemental reprocessing measures that might further reduce the risk of infection associated with the use of duodenoscopes, according to the American Hospital Association (AHA).

The new guidance came out shortly before news broke that Huntington Memorial Hospital in Pasadena, CA, is investigating a suspected pseudomonas bacteria outbreak related to duodenoscopes. Huntington Memorial said it discovered the potential problem in June during a review of lab samples, and it has reported three patient infections to health officials. Similar outbreaks of carbapenem-resistant *Enterobacteriaceae* (CRE) linked to duodenoscopes have been reported in North Carolina, Pittsburgh, Los Angeles, Chicago, and Seattle.

The new FDA measures, which emerged from an expert panel meeting led by the agency, are intended to supplement strict adherence to the manufacturer's reprocessing instructions, the AHA said. *(Recent research says bacteria survive on endoscopes even after a multi-step cleaning and disinfecting process. See story on that topic included in this issue.)*

The guidance says that implementing the measures requires specific resources, training, and expertise, which all healthcare

facilities might not have. "Therefore, it is critical that staff responsible for reprocessing duodenoscopes have the manufacturer's instructions readily available to promote strict adherence to the reprocessing instructions in the device labeling, understand the importance of their role in reprocessing the device, and maintain proficiency in performing these reprocessing tasks," the guidance states. "While the risk of infection transmission cannot be completely eliminated, the benefits of these devices continue to outweigh the risks in appropriately selected patients." *(Access the new guidance at http://1.usa.gov/1IFQO7F.)*

In February, the FDA issued safety recommendations to prevent possible microbial infections from reprocessed reusable duodenoscopes. *(Those recommendations can be accessed at http://1.usa.gov/1CNpAeh.)*

The FDA also has issued regulatory warnings that allege regulatory violations to three duodenoscope manufacturers, according to the AHA. The AHA said Olympus Corp. of the Americas and Hoya Corp. were cited for the following alleged violations:

- failing to report infections associated with their devices to FDA within 30 days;
- failing to adequately develop, maintain, and implement written Medical Device Reporting procedures.

Hoya also was cited for certain alleged violations related to design validation, corrective action, and process control, the AHA said. Fujifilm Medical Systems USA was cited for alleged violations related to design control, corrective action, inspection of parts, process validation, complaint handling, equipment testing, production processes, and device correction or removal, the AHA said.

The FDA letters asked the manufacturers to notify the agency within 15 days of the specific steps they have taken to correct the alleged violations. *(For more information on this topic, see these stories in* Same-Day Surgery*: "Culturing protocols devised for duodenoscopes to prevent CRE," May 2015, and "ECRI Institute's top patient safety concerns include scope reprocessing," June 2015.)*

Another recent development is the release of a standard from the Association for the Advancement of Medical Instrumentation (AAMI) titled "ANSI/AAMI ST91:2015, Comprehensive guide to flexible and semi-rigid endoscope processing in health care facilities."

AAMI said that there was no single document to turn to for guidance and existing resources sometimes contradicted each other. The new standard compiles all the information for processing flexible and semi-rigid endoscopes. It offers guidance on precleaning, leak-testing, cleaning, packaging, storage, high-level disinfecting, and sterilizing of flexible endoscopes. *(For ordering information, see Resource below. Also, the Association of periOperative Registered Nurses will release a "Guideline for processing flexible endoscopes" in January in the publication "Perioperative Guidelines for Practice.")*

RESOURCE

- **ST91** is available online for $195 list or $117 with AAMI member discount. The product code is ST91. Web: http://bit.ly/1i2peuX. ■

Scopes still contaminated after cleaning, study shows

Potentially harmful bacteria can survive on endoscopes, despite a multi-step cleaning and disinfecting process, according to a study published in the August issue of the *American Journal of Infection Control*, the official publication of the Association for Professionals in Infection Control and Epidemiology.

Although endoscopes were cleaned in accordance with multi-society guidelines, viable microbes and residual contamination remained on surfaces after each stage of cleaning, according to study findings.

Researchers from Ofstead & Associates in Saint Paul, MN, and Mayo Clinic in Rochester, MN, tested samples collected from 60 encounters with 15 colonoscopes and gastroscopes used for gastrointestinal procedures. The samples were tested after each reprocessing step to assess contamination levels. Investigators observed all reprocessing activities, and they used a checklist to ensure that cleaning protocols were performed according to published guidelines.

Reprocessing consisted of: bedside cleaning, manual cleaning in dedicated reprocessing rooms, and automated endoscope reprocessing with a high-level disinfectant. Disinfected endoscopes were stored vertically after drying with isopropyl alcohol and forced air. When contamination levels exceeded pre-determined benchmarks for each cleaning step, technicians went beyond guidelines and repeated cleaning procedures, and they retested after each attempt to reduce contamination.

Researchers performed microbial

cultures and various rapid tests to detect viable organisms and organic residue that remained after each step of cleaning.

Viable organisms were detected on 92% of devices after bedside cleaning; 46% after manual cleaning; 64% after high-level disinfection, and 9% after overnight storage. Rapid indicator tests detected contamination above benchmarks on 100% of devices after bedside cleaning; 92% after manual cleaning; 73% after high-level disinfection, and 82% after overnight storage.

"This study demonstrates that colonoscopes and gastroscopes can harbor residual organic material, including viable microbes, even when adherence with recommended reprocessing guidelines is verified," said the study authors. "More research is needed to identify processes that can ensure all flexible endoscopes are free of residual contamination and viable microbes prior to patient use, including the potential use of routine monitoring with rapid indicators and microbiologic cultures. Results from this study suggest that current standards and practices may not be sufficient for detecting and removing residual contamination."

The authors list several potential limitations of the study, including that it is a single-site study, and say it might not be generalizable nationwide. In addition, reprocessing technicians were aware of the researchers' use of a checklist to ensure guideline compliance and, therefore, might have devoted more time and effort to reprocessing. Another caveat is that technicians were informed immediately about contamination that exceeded benchmarks, and they repeated cleaning steps.

Recent reports of multidrug-resistant infections related to contaminated duodenoscopes, which have intricate elevator mechanisms and channels that are especially difficult to clean, have raised awareness about the necessity for meticulous reprocessing of all types of endoscopes to prevent the transmission of pathogens to patients. *(The study is available at http://bit.ly/1Ipiwpi.)* ■

SDS Manager

Warning signs: We're becoming more bureaucratic

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

One of the major reasons I changed my career path to developing outpatient service facilities outside of the mainstream hospital market was the refreshing attitude of "let's get it done."

At the time, both hospitals and freestanding surgery centers were driven to find a better way to process patients through the system. In a good way. The goal was to find a way to eliminate, as much as possible, the red tape associated with patient registration, waiting time, accommodations for friends and families, and everything that made the not-so-nice surgical process easier and friendlier for not only the patient and their loved ones, but for the staff and surgeons.

Such lofty aspirations.

It worked. Even die-hard critics will admit that we have improved our delivery of care, not just with the for-profit surgery centers, but also with hospitals. However, consider these areas:

• Patient satisfaction surveys.

How do we know we have improved? Look at responses to patient satisfaction surveys. Are you noticing a trend? I am.

Notice that, in the past, we allowed patient comments to address issues that were not in our selected list of questions from the companies that monitor patient responses. Are they slightly leading the patient to elicit a more favorable response so we look better than perhaps we are? I think so. You do know that you can tailor your questions that you want to ask the patients on these canned surveys.

• Patient registration.

At one time, we had cut down the patient registration to a reasonable time limit, and we did it with a smile. Think that is still the case? No. Don't believe me? Sit in your waiting room and watch what happens. We process people. That is not a compliment.

• Outsourced services.

The more we outsource our services — billing, management, pre-certification, follow-up phone calls — the more removed we become from our patients. I am a huge advocate of outsourcing, but not without oversight of the companies we use. Outsourcing does not diminish our responsibility for a good patient experience.

• Parking.

I loathe making our patients pay for parking on their day of surgery. I consider it cheap, unprofessional, and embarrassing for hospitals and surgery centers to charge patients to park to use their services.

I notice more and more freestanding surgery centers trying

to make a couple of extra bucks by mimicking hospitals that charge patients. What many people don't understand is that the service is usually an outside company that hospitals (and surgery centers) hire to provide this insulting service. While the hospitals get the flack for a few extra bucks per year, it is an outside company that makes all the money. It's a pet peeve of mine.

• Phone call the day of surgery.

Many facilities have stopped calling the patient after they have left the center the day of surgery. Yes, it costs a few bucks, but anyone can do it. It doesn't need to be a nurse. Just a simple call: "We just want to make sure you got home OK." It means a lot to the patients and to the loved ones with them. But, who makes time anymore for what they consider silliness?

• Your perception.

How did you feel after your day at work? Did you feel like you gave it your best, or did you just get through the day? I think the answer for a lot of us might be the latter.

How can you change this trend? Staff meetings. Ask your staff how you can improve your services. Some of these issues might come up and probably many more. Listen to them. Anything you can do is an improvement. Karma exists.

[Earnhart & Associates is a consulting firm specializing in outpatient surgery development and management. Earnhart & Associates' address is 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.] ■

Sleep apnea can pose malpractice risk

In 61 sentinel event reports, OSA was diagnosed or suspected

Surgical malpractice cases are increasingly citing obstructive sleep apnea (OSA) as a factor in the patient injury, according to a new study.

In the journal *Anesthesia & Analgesia*, **Dennis Auckley**, MD, of the MetroHealth Medical Center in Cleveland, OH, and colleagues reviewed three primary databases of legal literature to find cases in which patients with known or suspected OSA had adverse perioperative outcomes between 1991 and 2010. The article was published online ahead of print.

OSA had to be directly implicated in the outcome, and surgical mishaps such as uncontrolled bleeding were excluded. The adverse perioperative outcome had to result in a lawsuit that then was adjudicated in a court of law with a final decision rendered. There were 77,630 medical negligence cases in the time period studied. The researchers initially excluded 74,576 cases that were unrelated to OSA. Other cases eventually were excluded due to not being directly related to OSA, being non-surgical cases associated with OSA, involving pediatric cases, being settled out of court, or resulting from a surgical complication not related to OSA. The researchers found 24 cases, most occurring in or after 2007, for the final analysis.

Most of the operations (92%) were elective, and 71% of the overall group died. The researchers suspect that use of general anesthesia and opioids might have led to complications in 58% and 38% of cases, respectively. They also found that verdicts favored plaintiffs 58% of the time, with an average award of $2.5 million, ranging from $650,000 to $7.7 million.

Standardized screening tools for OSA should be used more extensively in surgery, the researchers suggest. OSA patients also might need special precautions postoperatively, they say. Some precautions include minimizing opioid use postoperatively, trying to keep patients off their backs, and providing additional monitoring for patients with known or suspected OSA. Patients also should be required to bring their at-home therapy, such as a sleep apnea mask, and use it at the hospital postoperatively, they say.

OSA affects about 5% of the population, but most cases are undiagnosed, the researchers note.

"Perioperative complications related to OSA are increasingly being reported as the central contention of malpractice suits. These cases can be associated with severe financial penalties," the researchers concluded. "These data likely underestimate the actual medicolegal burden, given that most such cases are settled out of court and are not accounted for in the legal literature."

An abstract of the study is available online at http://tinyurl.com/q5rxhqc.

The Joint Commission (TJC) has received 61 sentinel event reports in which the patient was diagnosed with or suspected of having OSA. OSA might have been a contributing factor

in some of these cases; however, the nature of OSA presents difficulties in directly associating OSA with the patient's death or injury, the TJC says.

The risk factors for OSA are obesity (BMI > 35), male gender, advancing age, craniofacial or upper airway soft tissue abnormalities, smoking, congestive heart failure, atrial fibrillation, nasal congestion, menopause, and family history, according to The Joint Commission, which quotes a study published in 2015.[1]

The Joint Commission reviewed root cause information for anesthesia-related events that resulted in death or permanent loss of function from 2004 through June 2015. Most events have multiple root causes. They included:

- anesthesia care, 67 events;
- assessment, 62 events;
- human factors, 61 events;
- communication, 58 events;
- leadership, 51 events;
- physical environment, 17 events;
- information management, 16 events;
- medication use, 16 events;
- continuum of care, 10 events;
- care planning, 10 events.

The reporting of most sentinel events to The Joint Commission is voluntary and represents only a small proportion of actual events. Therefore, these root cause data are not an epidemiologic data set, and no conclusions should be drawn about the actual relative frequency of root causes or trends in root causes over time, the TJC says.

TJC recommends that hospital and surgical facility staff take the following safety actions:[2]

• Screen and identify any patient suspected of having OSA.

According to the TJC, some OSA evaluation techniques organizations might want to consider include: Epworth Sleepiness Scale, or ESS (http://bit.ly/1UdFXHF), STOP-BANG Questionnaire (http://www.stopbang.ca/screen.php), Apnea Risk Evaluation System, or ARES (http://bit.ly/1NInPFW), or Berlin questionnaire (http://1.usa.gov/1UdG0mI).

• Evaluate the patient's plan of care to ensure all precautions are taken while in your facility.

This evaluation includes assessing the use of sedating medications and narcotics, continuous pulse oximetry monitoring of the patient in an observed environment, use of supplemental oxygen or positive airway pressure device, and patient positioning.

• Use guidelines for the use of anesthesia with suspected OSA patients.

TJC reports that you can use the following:[3]

— For pediatric patients, follow The American Academy of Pediatrics (AAP) revised guidelines for managing and monitoring sedation.

— For adult patients with known OSA, follow the recommendations of the American Society of Anesthesiologists 2006 Task Force.[4]

"Be aware that intermittent pulse oximetry or continuous bedside oximetry without continuous observation does not provide the same level of safety," TJC says.

REFERENCES

1. Strohl KP. Overview of obstructive sleep apnea in adults. *UpToDate* 2015. Accessed at http://bit.ly/1EWZKUA.
2. The Joint Commission. At risk: Obstructive sleep apnea patients. *Quick Safety* 2015. Accessed at http://bit.ly/1SK5tFt.
3. Academic Medical Center, Patient Safety Organization. *Patient Safety Alert: Obstructive sleep apnea — Management considerations* 2013; 19. Accessed at http://bit.ly/1fGQnSj.
4. American Society of Anesthesiologists. Practice guidelines for the perioperative management of patients with obstructive sleep apnea. A report by the American Society of Anesthesiologists Task Force on Perioperative Management of Patients with Obstructive Sleep Apnea. *Anesthesiology* 2014; 120(2):268-286. ■

Anesthesia staff key to identifying children at risk for sleep-disordered breathing prior to surgery

Knowing which risks might come into play before or during surgery is especially important where children are concerned. Implementation of a screening questionnaire detailed in the August 2015 *AANA Journal* helps anesthesia professionals identify children with symptoms of sleep-disordered breathing (SDB) before undergoing a general anesthetic.

The article, "Snoring, trouble breathing, un-refreshed (STBUR) screening questionnaire to reduce perioperative respiratory adverse events in pediatric surgical patients:

A quality improvement project," appears in the journal, published by the American Association of Nurse Anesthetists.

A primary challenge to addressing SDB in children about to undergo surgery is the lack of awareness of the risks and parents who underestimate their child's condition. "Parents are often unaware of the potential problems related to their child's snoring. Recognition of this condition is of utmost importance, as children have died after routine tonsillectomies after receiving too much pain medication," says lead author **Karrey L. Terry**, CRNA, DNP, an assistant professor at the University of Colorado School of Medicine and staff nurse anesthetist at Children's Hospital Colorado in Denver. At the time of this project, she was a doctorate of nursing practice student at the University of Colorado College of Nursing.

Because SDB manifests itself in a patient's respiration, anesthesia professionals are in a perfect position to uncover undiagnosed conditions such as SDB before surgery to head off respiratory complications during anesthesia. The STBUR questionnaire provides five questions that help to identify SDB prior to surgery. They are:

- Does your child snore more than half the time?
- Does your child snore loudly?
- Does your child have trouble breathing or struggle to breathe?
- Does your child ever stop breathing during the night?
- Does your child wake up feeling unrefreshed?

The importance of identifying those at risk is paramount: The likelihood of developing a perioperative respiratory adverse event increases threefold in the presence of any three STBUR symptoms and by tenfold when all five symptoms are present.

Including the STBUR questionnaire in the pre-anesthesia interview serves to raise awareness of potential risks and allows anesthesia professionals to modify their airway and anesthesia plans toward safer practices.

"We are looking to improve safety by creating evidence-based standards of care," says Terry.

For more information on the STBUR questionnaire and the *AANA Journal* article, visit http://www.aana.com/sdb-patients. ■

Newly released research identifies cause of postoperative delirium in older patients

Newly published research from the Department of Geriatrics and Gerontology at the Rowan University School of Osteopathic Medicine in Stratford, NJ, explains why up to half of older adults who undergo general anesthesia develop postoperative delirium, which is the sudden onset of confusion, aggression, or agitated behavior that could progress to dementia. The findings indicate that older patients who are undergoing surgery might benefit from a less-potent, slower-acting anesthetic.

Working with animal models, the research team tested two inhaled anesthetics: sevoflurane and isoflurane. Sevoflurane is one of the commonly used inhaled anesthetics for inducing general anesthesia because it acts more quickly and has a shorter recovery time. However, the researchers found that sevoflurane caused increased disruption of the blood-brain barrier, the cellular structure that regulates the entry and removal of various blood components in the brain. Isoflurane, however, failed to demonstrate similar levels of blood-brain barrier breach.

"Our research has shown that when the blood-brain barrier breaks down, various plasma components, such as immunoglobulin, gain access into the brain and selectively bind to pyramidal neurons," said lead author **Nimish K. Acharya**, PhD, at the Biomarker Discovery Center, New Jersey Institute for Successful Aging, Rowan University School of Osteopathic Medicine, and Department of Geriatrics and Gerontology, both at the Rowan University School of Osteopathic Medicine. "This may disrupt normal neuronal activity and could cause the onset the symptoms that define postoperative delirium."

The selective binding of those autoantibodies to the pyramidal neurons that dominate the cerebral cortex occurred in animals treated with both inhaled anesthetics. However, older animals treated with sevoflurane showed a "dramatic and significant increase in the density and extent of vascular leak" caused by a disruption in the blood-brain barrier. By contrast, older animals exposed to isoflurane failed to show any significant age-related differences in the density or extent of vascular leaks.

The study's corresponding author, **Robert Nagele**, PhD, director of the Biomarker Discovery Center and a professor of medicine, both

at the Rowan University School of Osteopathic Medicine, said, "Extrapolating this data to humans suggests that older patients who will be exposed to inhaled anesthetics during surgery would benefit from a less potent anesthetic that would presumably pose less risk of blood-brain barrier compromise and minimize the risk of subsequent postoperative delirium." The authors of the study suggest that more research is needed to identify other anesthetics for use in surgery that would be less disruptive to the blood-brain barrier and less likely to lead to postoperative complications such as delirium, cognitive decline, and dementia. This study, which appears online in *Brain Research*, was supported by funding from the Osteopathic Heritage Foundation.

To access the study, go to http://bit.ly/1KQISRH. ■

Anesthesia info management system alerts can boost patient care, but raise implementation challenges

Automated alerts generated using data from anesthesia information management systems (AIMS) are a promising approach to influencing the behavior of anesthesia providers, with the goal of improving care for patients undergoing surgery, according to a paper published in the September 2015 issue of *Anesthesia & Analgesia*.

However, developers must address a wide range of issues and concerns to ensure that alerts are reaching the right people, at the right time, to be effective in producing the desired changes, wrote **Richard H. Epstein** of Sidney Kimmel Medical College at Thomas Jefferson University, Philadelphia, and colleagues.

Modern AIMS routinely collect a vast amount of data on patient status and patient care. Clinicians and researchers are interested in mining these data to develop alert systems to improve key aspects of patient care and monitoring during surgery. Studies have shown that such anesthesia clinical decision support (CDS) systems can increase adherence to protocols and improve financial performance, but have yet to demonstrate improved clinical outcomes.

Designing and implementing such systems entails a "multitude of concerns" that must be recognized and addressed, to produce the desired effects. To illustrate these complexities, Epstein and coauthors shared their experience in developing two CDS interventions using AIMS data. The first case example concerns an effort to reduce fresh gas flow rates when using inhaled anesthetics. That reduction is important not only for cost control, but also to reduce the environmental impact of gases ventilated to the atmosphere.

In this case, a "post-hoc" approach was deemed an appropriate first step. An automated system was designed in which each anesthesiologist received a monthly email providing feedback on flow rates over his or her 10 most recent cases. On evaluation, fresh gas flow rates decreased significantly from before to after the alert system was implemented.

Other situations call for more immediate feedback to achieve the desired improvement. That's illustrated in the second case example: an effort to reduce gaps in routine blood pressure (BP) during surgery. While measuring BP every five minutes is the standard, gaps of 10 minutes or longer are common.

This case required a "near real-time" approach, with alerts sent directly to the operating room workstation where the patient's condition was being recorded. Evaluation found that the targeted improvements in BP monitoring were met, once alert intervals were decreased to six minutes. Over four years' follow-up, the number of weekly alerts remained about the same, which suggested a "lack of long-term learning" and highlighting the need to continue the alert system.

Alert systems should not be implemented until their usefulness is confirmed, Epstein and colleagues emphasized. For example, they considered sending near real-time alerts regarding drops in blood oxygenation level, but found that most such episodes resolved within minutes, before the alert could be sent. "Lack of utility should be assumed until testing shows otherwise, even if a benefit seems

COMING IN FUTURE MONTHS

- Reducing OR turnover times
- Need to recruit periop nurses? We have ideas
- Reduce your risk of fires
- Surgical site infections can be cut: We tell you how

apparent," the researchers wrote.

Other concerns include possible unintended consequences of alert systems. For example, one study suggested that CDS reminders were leading to overuse use of anti-nausea drugs. Potential regulatory issues must be considered, such as the risk of running afoul of FDA rules on the use of CDS software or mobile devices. The authors also touch on the technical challenges of implementing and maintaining alert systems.

Although data collected by AIMS provide the opportunity to improve patient care in many ways, careful forethought and follow-up are needed to ensure that alerts are well-designed and effective, Epstein and coauthors said. "Our goal is to inform developers and users of CDS for AIMS about the multitude of concerns they should consider during development and implementation to increase effectiveness and mitigate potentially disruptive aspects of this technology," they said. ■

SAGES launches program to reduce bile duct injury

The Society of American Gastrointestinal and Endoscopic Surgeons (SAGES) is educating practicing surgeons, residents, and fellows about technical steps to prevent bile duct injury, such as the Critical View of Safety and intraoperative biliary imaging.

Bile duct injury can be a devastating complication of cholecystectomy. It has been reported to occur in 0.2 to 1% of laparoscopic cholecystectomies.

According to **Michael Brunt**, MD, SAGES president, "After 25 years of laparoscopic cholecystectomy, it is time to undertake the difficult issue of reducing bile duct injuries for this common procedure."

The SAGES resources include strategies for minimizing injuries and a video by Brunt introducing the SAGES Safe Cholecystectomy program. To access, go to http://www.sages.org/safe-cholecystectomy-program.

The SAGES Safe Cholecystectomy Task Force also plans to support surgical decision-making around the timing of surgery for acute cholecystitis and the management of various difficult cholecystectomy scenarios. ■

Electronic Health Fairness Act passes Senate

The U.S. Senate recently passed the Electronic Health Fairness Act of 2015 (S 1347), according to the Ambulatory Surgery Center Association (ASCA). This legislation protects physicians practicing in ASCs from meaningful use penalties in the Medicare program until a certified electronic health record technology (CEHRT) is available for the ASC setting. Similar legislation passed the U.S. House of Representatives in June.

ASCA worked closely with ASC champions Sen. Johnny Isakson (R-GA) and Sen. Michael Bennett (D-CO) on this legislation in the Senate, and members built support in Congress to achieve final passage.

Next, the House and Senate must reconcile slightly different legislation into one cohesive bill. *(To access the Senate bill, go to http://1.usa.gov/1hfTeD3.)* ■

Free infographic on robotics

A free infographic, *Robotic Surgery,* from ECRI Institute in Plymouth Meeting, PA, gives a view of the marketplace and shows purchasing trends, major procedure types, and information on future robots. Topics also include:

- average quoted prices and key features of da Vinci Xi, Si, and Si-e models;
- safety recommendations and adverse events related to surgical robots;
- guidance on surgeon training, credentialing, and privileging.

Download the infographic at www.ecri.org/robotinfo. ■

CNE/CME OBJECTIVES

After reading *Same-Day Surgery,* the participant will be able to:

- identify clinical, managerial, regulatory, or social issues relating to ambulatory surgery care;
- identifiy how current issues in ambulatory surgery affect clinical and management practices;
- incorporate practical solutions to ambulatory surgery issues and concerns into daily practices.

SAME-DAY SURGERY

CNE/CME 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. Scan the QR code to the right or log on to the AHCMedia.com site to take a post-test. Go to "My Account" to view your available CE activities. First-time users will register on the site using the subscriber number on their mailing label, invoice, or renewal notice.
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 successfully completing the test, your browser will be automatically directed to the activity evaluation form, which you will submit online.
5. A credit letter will be e-mailed to you instantly.

CNE/CME QUESTIONS

1. **What was the outcome of the case of the employee who was about to be fired and sent emails from her work computer to her personal email, including highly sensitive patient files?**

   A. She was protected because she had worked at home and transferred patient files to her personal email previously.
   B. She was protected by statements in the employee handbook.
   C. She was found guilty on all seven counts of computer fraud.

2. **Because all healthcare facilities might not have the specific resources, training, and expertise to implement new reprocessing measures from the FDA, what should be done by staff responsible for reprocessing duodenoscopes, according to the agency?**

   A. Have the manufacturer's instructions readily available to promote strict adherence to the reprocessing instructions in the device labeling
   B. Understand the importance of their role in reprocessing the device
   C. Maintain proficiency in performing these reprocessing tasks
   D. All of the above

3. **According to a study in the *American Journal of Infection Control,* although endoscopes were cleaned in accordance with multi-society guidelines, viable microbes and residual contamination remained on surfaces after what?**

   A. Bedside cleaning
   B. Manual cleaning in dedicated reprocessing rooms
   C. All stages of cleaning

4. **In a study in which researchers reviewed three primary databases of legal literature to find cases in which patients with known or suspected OSA had adverse perioperative outcomes between 1991 and 2010, what percentage of the cases were elective?**

   A. 5%
   B. 27%
   C. 54%
   D. 92%