SAME-DAY SURGERY

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

JANUARY 2015 Vol. 39, No. 1; p. 1-12

INSIDE

Enclosed in this issue:

- Results of *2014 Salary Survey*
- **Online issue:** *Infection Control Breach Reporting Policy and Procedures*

AHC Media

Data breach at spine center raises question: How do you prevent it?

Former employee took personal information from 12,000 patients

Personal information from about 12,000 patients was taken from a Las Vegas-based brain and spine surgery center in 2011-2012 and discovered earlier this year. An ex-employee stole names, addresses, birthdates, Social Security numbers, and patient billing account numbers from Western Regional Center for Brain & Spine Surgery, according to the center. The former employee is being investigated by law enforcement for using the information for fraudulent purposes.

The center was notified about the breach in May by law enforcement. The breach occurred in 2011 and 2012, according to the Department of Health and Human Services. The center notified all patients who were potentially affected, and it is reviewing its technology safeguards, as well as its internal policies and procedures, according to a letter posted for patients. In the letter, **Robin Hasty**, office administrator, said, "Presently, we are unable to identify the specific patients whose personal health information was actually stolen nor do we know which of those patients whose information was stolen was also used for fraudulent activities. We are therefore notifying all patients whose personal information was in our billing system at the time of the breach." *(To see the entire letter, go to http://bit.ly/11Lk4vv.)*

Insider threats are more common than you might think. One survey of 419 enterprise-security staff members indicated 23% of enterprises have

Financial Disclosure: Executive Editor Joy Dickinson and Board Member and Columnist Stephen W. Earnhart report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study. Board Member and Nurse Planner Kay Ball reports that she is a stockholder with Steris Corp,, she is on the speakers bureau for Ethicon Endosurgery, and she is a retained consultant with Mobile Instrument & Service, IC Medical, and Megadyne. Mark Mayo, consulting editor, reports that he is executive editor of Golf Surgical Center in Des Plaines, IL. Robert S. Bray Jr., MD, physician reviewer, discloses that he is a stockholder with RSB Spine and with DISC Integrated Medical Group. Damian Capozzola, Jamie Terrence and Tim Laquer, guest columnists, have no relevant relationships to disclose.

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, call Tria Kreutzer at (404) 262-5482. 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: AHC Media, LLC is accredited as a provider of CNE by the American Nurses Credentialing Center's Commission on Accreditation. This activity has been approved for 16.4 nursing contact hours using a 60-minute contact hour. Provider approved by the California Board of Registered Nursing, Provider #14749, for 16.4 Contact Hours. AHC Media, LLC is accredited by the Accreditation Council for Continuing Medical Education to provide CME for physicians. AHC Media, LLC designates this enduring material for a maximum of 21 *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 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 joy.dickinson@ahcmedia.com. (404) 262-5410
DIRECTOR OF CONTINUING EDUCATION AND EDITORIAL: Lee Landenberger.

experienced data breaches that were insider-driven.[1] The survey was conducted by SpectorSoft, a Vero Beach, FL-based provider of monitoring and analysis software for computers and mobile devices. The survey included 419 respondents from enterprise and government agency organizations. In that survey, 47% of respondents reported that former employees took information with them when they left the company. **Mark Mayo**, executive director of the ASC Association of Illinois and principal, Mark Mayo Health Care Consultants in Round Lake, IL, says, "The point here is if it can happen to them, it can happen to you, so it's a matter of when, not if, and the 'when' will happen sooner if you do not take action."

Another study released in June says, "The occurrences of ex-employees continuing to access their systems from their former jobs are rampant, and without the proper restrictions or monitoring in place IT people could be completely oblivious."[2] The publisher of the study is IS Decisions, based in Biarritz, France, which focuses on IT safeguards and security. Nearly one in 10 (9%) ex-employees are going into their former employers' systems, the report says. "This represents a considerable risk, especially given that ex-employees are far more likely to have malicious intentions and a lot less incentive to consider the sensitivity of the business' data," IS Decisions says.

The repercussions can be serious, including violations of the Health Insurance Portability and Accountability Act (HIPAA), says **Reece Hirsch**, JD, partner in Healthcare Practice and a co-head of Privacy and Cybersecurity Practice at Morgan, Lewis & Bockius in San Francisco. "HIPAA imposes a range of penalties, from $100 per violation to $50,000 per violation," Hirsch says. "But a poorly handled breach can lead to a host of negative consequences for [providers] beyond HIPAA penalties, including regulatory enforcement action, class action lawsuits, civil lawsuits under state law causes of action, and, perhaps most importantly, damage to patient relationships and reputation."

But can you stop a breach? Probably not, say sources interviewed by *Same-Day Surgery*. **Stephen Trosty**, JD, MHA, ARM, CPHRM, president of Risk Management Consulting in Haslett, MI, says, "If someone is smart enough about computers and determined to breach data, it probably is possible for this to occur."

Hirsch says that usually the system security for an outpatient practice isn't "strong enough to

EXECUTIVE SUMMARY

A former employee took personal information from about 12,000 patients at a Las Vegas-based brain and spine surgery center and is being investigated for using the information for fraudulent purposes. To avoid this situation:

- Create a culture of privacy compliance, including no password sharing.
- Consider a policy to prohibit downloading medical information to a laptop or external device. Encrypt all data.
- Limit access to data to those who absolutely must have it, and track access.
- Enforce password complexity. *(See "Passwords Are Like Underwear," p. 3.)*

withstand the most sophisticated external threats, and it is very difficult to stop an employee who sets out to intentionally disclose or sell medical information." However, your facility should have a reasonable breach response plan that fulfills the requirements of the HIPAA Breach Notification Rule, he says.

Trosty adds that "there are things that can be done to try to prevent this from happening or to make it more difficult for someone to succeed." Consider these suggestions:

• Create a culture of privacy compliance.

What's the best thing you can do? According to Hirsch, "create a culture of privacy compliance within the organization."

"That means training personnel to recognize a potential security breach when they see the signs of one, whether that breach originates from a hacker in China or the co-worker at the next workstation," he says.

Also, address password sharing, which younger employees often have a blasé attitude toward, IS Decisions says. Make sure employees know that password sharing isn't condoned, even with managers.

Educate staff about why internal security threats are at least as threatening as external ones, the company says. "This will mean an ongoing commitment to staff training and education, not a 'tick-box' approach which we know does not work in ensuring staff take on the message and remember," IS Decisions says.[2] Managers lead by example, particularly when it comes to expecting employees to share passwords, the company says. "Not sharing your password is not a matter of trust, it is a matter of course," it says.

• Examine your policy on downloading medical information.

If feasible, consider a policy to prohibit downloading medical information to a laptop or external device, Hirsch advises.

"If it's necessary for medical information to be stored on laptops, encryption of laptops is definitely a best practice," he says. "If a practice uses encryption that meets [the Department of Health and Human Services'] standard identified in the HIPAA Breach Notification Rule, then disclosure of that encrypted data will not constitute a 'breach,' as defined."

More than 73% of the breaches serviced by Beazley Breach Response (BBR) Services in 2013 involving portable devices could have been prevented if the devices were encrypted. BBR is an Atlanta company providing breach response insurance.

Encrypt all data at all times, Trosty says. "The encryption should extend to all sensitive and related data, and must exist for both internal and external transfer and access to data," he says. Don't use the same encryption for internal and external transfer of data, he advises, and this position should apply to all entities and individuals to whom data will be shared or transferred. "Sending and receiving of data should require a password, in addition to the encryption," Trosty says. "That can help limit unauthorized access and allow for any necessary tracking."

• Enforce password complexity.

Computer systems can systematically cycle through all permutations of potential passwords, says BBR. Do not allow passwords that are easy to crack, it says; dictionary words are capable of being deduced with an algorithm. *(See "Passwords Are Like Underwear, above.)*

Trosty says, "Each person who has access to any data should have a password that controls both access to information, as well as to specific information."

This password should preclude access to other data, he says. "The password should only be good for a set period of time and should periodically be changed to help prevent others from learning the password and using it, as well as to continue to ensure that access to specific data and information continues on a need-to-know basis," Trosty says.

When an employee changes jobs, review and make changes to access if needed, he says. When an employee leaves a facility, permanently block that password from access to any information, Trosty says. "This is possible to do and can be done by the IT personnel," he says. "This password should not again be used."

Mayo suggests that if a key employee, such as someone who works in information technology, leaves, especially if an employee is fired or retires, "then you may want to hire an outside tech firm to make sure that any potential electronic backdoors have been removed to prevent a former employee from re-entering the system even if you have removed that person's frontdoor access codes."

• Limit access to data, and track access.

Passwords Are Like Underwear

- Change yours often.
- Don't share them with friends.
- The longer, the better.
- Be mysterious.
- Don't leave yours lying around.

Source: IS Decisions, Biarritz, France. Web: http://www.isdecisions.com/insider-threat-persona-study.

Limit access to data to those who absolutely have a need to access it, Trosty says.

"This should be data-specific, since few employees have the need to access all patient or other data," he says. "It should be limited to what is needed to do one's job."

Also, have a system to trace entry into the data, Trosty says. "It should be possible to learn who accessed data and when it was done," he says. "This can be done." Also, if possible, have a process to alert the appropriate person if access is attempted by someone who doesn't have clearance, Trosty says. *(For information about an FBI warning on computer hackers, see story, below.)*

REFERENCE

1. SpectorSoft. *Insider Threat: Alive and Thriving.* April 24, 2014.
2. IS Decisions. *From Brutus to Snowden — A Study of Insider Threat Personas.* Accessed at http://www.isdecisions.com/insider-threat-persona-study.

RESOURCE

- The American Hospital Association has created a cybersecurity page. Web: http://www.aha.org/advocacy-issues/cybersecurity.shtml. ■

FBI warns healthcare companies of hacker threat

The FBI has warned healthcare industry companies that they are being targeted by hackers, following a successful attack on Community Health Systems in Franklin, TN, that resulted in the theft of millions of patient records.

"The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)," the agency said in a *Flash* alert sent to healthcare providers. "These actors have also been seen targeting multiple companies in the healthcare and medical device industry typically targeting valuable intellectual property, such as medical device and equipment development data," the alert said.

The FBI and Department of Homeland Security periodically release alerts to provide U.S. businesses with technical details and other information they can use to prevent or identify cyber attacks. The reports typically are issued only to businesses.

In April 2014, the FBI warned the healthcare industry that its systems were lax compared with other sectors, which makes it vulnerable to hackers looking to access bank accounts or obtain prescriptions. ■

Corporate negligence can complicate med mal

Claims of corporate negligence can increase the stakes in a malpractice case, as plaintiffs seek the deeper pockets of the employer who hired and allowed a supposedly deficient healthcare provider to injure a patient.

Corporate negligence claims demonstrate the power of a plaintiff to widen the scope of a malpractice case beyond the physician and the physician's insurer, says **Matthew L. Kinley**, JD, a partner at the law firm of Tredway Lumsdaine & Doyle in Los Angeles. The usual claim is that the facility or health system should have known the physician was unqualified in some way and should pay for allowing him or her to practice.

A current example is the case of Christian Schlicht, MD, a physician hired by the Gerald Champion Regional Medical Center in Alamogordo, NM. According to a press release from the 65-year-old hospital, the board of directors authorized a bankruptcy filing to ensure the hospital's ability to provide critical healthcare services while creating an orderly process to resolve lawsuits in a fair and timely manner.

Trial proceedings recently began for 71 plaintiffs suing Quorum Health Resources, a hospital administration company based in Brentwood, TN, that provided top executives and physicians for the hospital. At issue is whether the hospital and Quorum were negligent in hiring Schlicht and allowing him to continue operating even after they were alerted that he was performing experimental spinal surgery with devastating results.

Attorneys for the plaintiffs are alleging corporate negligence and claiming the employer and Quorum knew the doctor was performing a spinal procedure, not approved by the Food and Drug Administration, that involved bone cement. In opening arguments, one plaintiff's attorney noted that the procedure was not allowed anywhere in the world and said it amounted to "absolute human experimentation." Schlicht

was performing that procedure and others considered just as risky and unsuccessful up to a week before he quit his $450,000 job at the hospital.

Quorum contends that the hospital's board of directors was liable for the damage Schlicht caused and that medical staff members were responsible for supervising surgeons. The plaintiffs counter that the company should never have hired the surgeon and knew about his repeated failures with experimental surgery.

"These cases can get quite complicated because you get into asking, what is the role of the trustees, the board of directors, and the medical staff?" Kinley says. "Corporate negligence also can involve situations like a piece of equipment failing at a critical time. The question then is whether the [facility] had policies and procedures in place to respond to that failure in the appropriate way."

A facility can be found negligent for failing to monitor the history of equipment failures and repairs and for failing to replace defective or aged and unreliable equipment, says **Mark Mayo**, executive director of the ASC Association of Illinois and principal, Mark Mayo Health Care Consultants in Round Lake, IL.

In years past, corporate negligence was more difficult to prove in a straight medical malpractice case because the physician generally was considered to be the "captain of the ship" in every way, with ultimate liability falling there, Kinley says. That theory has shifted now so that facilities and health systems have much responsibility to credential, privilege, and monitor physicians and more liability if they fail to do so. That responsibility is partly because healthcare employers have so many more resources now for investigating the background and training of physicians, Kinley notes. Failure to check the National Practitioner Data Bank, for example, would be seen as a major oversight by the employer, he says.

In addition, courts and juries now expect employers to monitor the performance of physicians by randomly auditing patient records and reassessing performance at regular intervals, Kinley explains. Not committing fully to that oversight can lead to large jury awards. "The courts have ruled that juries get to look at different things in determining the standard of care. So if you have a risk management policy about how and when you are supposed to review physicians, and you didn't, that is almost negligence per se," Kinley says. "Be aware that a jury is going to be looking at your rules and regulations to determine if you met your own standards of care." ■

EXECUTIVE SUMMARY

Corporate negligence is a common claim used by plaintiffs in medical malpractice cases. Successful use of this strategy will make the facility or health system liable for what otherwise could have been attributed to an individual.

- A current case involves claims of corporate negligence for allowing a surgeon to perform allegedly experimental spine procedures.
- Equipment failures also could lead to corporate negligence claims.
- Legally, the surgeon is no longer the "captain of the ship."

E. coli outbreak at Illinois hospital tied to contaminated specialized GI scopes

Despite no lapses in the disinfection process recommended by the manufacturer being identified, duodenoscopes had bacterial contamination associated with an outbreak of a highly resistant strain of *Escherichia coli,* commonly known as *E. coli*, at a hospital in Illinois, according to a study in the Oct. 8 *JAMA*, a theme issue on infectious disease.

The duodenoscope is different than the scope used for routine upper gastrointestinal endoscopy or colonoscopy. The procedure linked with these specialized scopes is endoscopic retrograde cholangiopancreatography (ERCP), a medical procedure that allows doctors to diagnose and treat life-threatening problems in the bile and pancreatic ducts.

Carbapenem-resistant Enterobacteriaceae (CRE) are multidrug-resistant organisms isolated predominantly from patients with exposures in healthcare facilities. CRE are a public health concern because treatment options are limited and invasive infections are associated with a risk of death.

The New Delhi metallo-beta-lactamase (NDM) is a carbapenemase, which is an enzyme that breaks down antibiotics, which has been infrequently reported in

the United States. However, NDM-producing CRE have the potential to add substantially to the total CRE burden. Understanding transmission and preventing further spread of CRE is a public health priority, according to background information in the article.

In March 2013, NDM-producing *E. coli* was identified from a patient at a teaching hospital in Illinois. Between March 2013 and July 2013, six additional patients with a history of admission to this hospital had positive clinical cultures for NDM-producing *E. coli*. In August 2013, Lauren Epstein, MD, MSc, an Epidemic Intelligence Service officer at the Centers for Disease Control and Prevention, and colleagues launched an investigation to identify the source and prevent further NDM-producing CRE transmission at this hospital. Interviews were conducted with healthcare personnel at the hospital.

A medical record review revealed that a history of ERCP procedures involving the use of a duodenoscope was common among initial cases. In this outbreak, 39 patients with NDM-producing CRE were identified from January 2013 to December 2013. Thirty-five had duodenoscope exposure in one hospital. Some of those patients had positive blood cultures, which often is an indication of infection, and others were found to be colonized with CRE but did not have an infection with CRE.

NDM-producing *E. coli* was recovered from a reprocessed duodenoscope and shared similarity to all case patient isolates. Based on a case-control study, case patients had significantly higher odds of being exposed to a duodenoscope. The authors write that the large number of exposed patients who ultimately had NDM-producing CRE isolated from clinical or screening cultures suggests that duodenoscopes were an efficient source of transmission.

An infection prevention assessment that focused on duodenoscope reprocessing was conducted, and it was found that the hospital followed all manufacturer-recommended procedures. After the hospital changed its duodenoscope reprocessing to gas sterilization, no additional case patients were identified.

"The complicated design of duodenoscopes makes cleaning difficult. It appears that these devices have the potential to remain contaminated with pathogenic bacteria even after recommended reprocessing is performed," the researchers write.

They add that another option for ensuring adequate duodenoscope reprocessing might be to conduct testing for residual contamination during reprocessing.

"Many international professional societies recommend periodic microbiological surveillance testing of duodenoscopes after full reprocessing," the researchers write. "Facilities should be aware of the potential for transmission of antimicrobial-resistant organisms via this route and should conduct regular reviews of their duodenoscope reprocessing procedures to ensure optimal manual cleaning and disinfection." ■

CMS memo to surveyors leads to ASC policy — Surveys targeting infection control breaches

With reports that the Centers for Medicare & Medicaid Services (CMS) told its surveyors to contact public health departments immediately if they see flagrant breaches of infection control, one surgery center has developed a new policy and procedure on infection control breaches.

CMS sent a memo to surveyors and listed concerns about unsafe injection practices and improper use of medication vials.[1] The guidelines in the memo were effective May 30, 2014. *(For more on the memo, see "CMS sounding alarm: unsafe needle practices — Specific reference made to ASCs and hospitals,"* Same-Day Surgery*, September 2014, p. 91. To access the memo, go to http://go.cms.gov/1vlKKKw.)*

"Upon reading the CMS memo, our team created a policy that says we will work cooperatively with state and accrediting organizations in identifying and monitoring any breaches and including the breaches listed in the CMS memo," says **Mark Mayo**, CASC, executive director of Golf Surgical Center, Des Plaines, IL. [*The policy is included in this month's online issue of* Same-Day Surgery. *To access, go to www.ahcmedia.com and select "Access Your Newsletters." You'll need your customer number from your mailing envelope or your invoice. For assistance, contact customer service at (800) 688-2421 or customerservice@ahcmedia.com.]*

The following breaches were listed in the CMS memo:

- using the same needle for more

than one individual;

• using the same (pre-filled/manufactured/insulin or any other) syringe, pen, or injection device for more than one individual;

• re-using a needle or syringe that already has been used to administer medication to an individual to subsequently enter a medication container (e.g., vial, bag), and then using contents from that medication container for another individual;

• using the same lancing/fingerstick device for more than one individual, even if the lancet is changed.

In the facility's policy, Mayo referenced the importance of strictly adhering to the "One Needle/One Syringe /One Time" nationally recognized practice that is part of the "One & Only" campaign from the Centers for Disease Control and Prevention. *(For more on the campaign, go to http://www.cdc.gov/injectionsafety/1anOnly.html.)*

REFERENCE

1. Centers for Medicare and Medicaid Services. *Infection control breaches which warrant referral to public health authorities.* May 30, 2014. Web: http://go.cms.gov/1vlKKKw.

GUEST COLUMN

State supreme court affirms $4.4 million verdict based on lack of informed consent

*By **Damian D. Capozzola**, Esq.*
Law Offices of Damian D. Capozzola
Los Angeles

***Jamie Terrence**, RN*
President and Founder, Healthcare Risk Services
Former Director of Risk Management Services (2004-2013)
California Hospital Medical Center
Los Angeles

***Tim Laquer**, 2015 JD Candidate*
Pepperdine University School of Law
Malibu, CA

An otherwise healthy adult man fell from a ladder in December 2009. He suffered multiple non-displaced rib fractures as well as other injuries, and he sought treatment at a nearby hospital. The patient suffered from severe chest pain despite having received an oral pain medication.

The patient's physicians requested a consult from a thoracic surgeon associated with the hospital who performs a special pain-relief procedure known as the "On-Q procedure." This procedure involves the insertion of a 5 inch long catheter, which contains several holes, under the patient's skin and over the ribs using a metal tunneling device. After the catheter is in place, a liquid analgesic runs through it and soaks the surrounding tissue and nerves. This process allows for continuous distribution of the analgesic and allows relief from pain associated with the rib fracture. The On-Q procedure has not been approved by the Food and Drug Administration (FDA) and is thus an "off-label" use of the On-Q catheter.

During the consult, the surgeon discussed the procedure with the patient, including the aim of pain relief and risks of bleeding, infection, and injury to adjacent organs or tissues. The surgeon also discussed alternatives. During trial, he testified that he normally informed patients that epidural anesthesia was a very effective alternative, but it was not an option because it has risks and limitations. The patient was not given the choice of having epidural anesthesia.

Furthermore, the surgeon completely failed to disclose his own personal financial interest in the On-Q procedure. Two years prior, the surgeon entered into a contract

EXECUTIVE SUMMARY

A patient was admitted to a hospital for non-displaced rib fractures. He experienced severe chest pain, despite receiving oral pain medication. The physicians requested a consult from a thoracic surgeon who performs an "On-Q procedure."

- The surgeon failed to advise the patient that he had a financial interest in the procedure based on a contract with the On-Q's manufacturer. The surgeon never gave the patient the option to receive an epidural instead.
- The patient underwent the procedure but suffered from complications that required significantly more time in the hospital and several more surgeries.
- The patient sued the surgeon and hospital. The jury found both liable and awarded $4.4 million in damages.

with the On-Q's manufacturer to give presentations and promote the procedure. The surgeon's performance of the procedure increased significantly, and he received approval from the hospital to study the procedure.

The patient agreed to and underwent the procedure, but difficulties quickly followed. The day after insertion, the patient inadvertently removed the catheters, which necessitated the insertion of two new catheters. One of these subsequent catheters became displaced and perforated the patient's internal organs, and the patient underwent several surgeries to remove the catheter and repair the organ damage.

After the ordeal, the patient brought suit against the surgeon and hospital. He alleged multiple bases for negligence. He claimed the surgeon failed to obtain informed consent and negligently performed the procedure. He claimed that the hospital was liable because the surgeon was its agent, along with the hospital's negligent management of the surgeon's On-Q study and negligent "expedited review" of the surgeon's application to conduct the study. Following an eight-day trial, the jury returned a verdict for the plaintiff and awarded $3.75 million in damages to the plaintiff plus $650,000 to the plaintiff's wife for loss of consortium.[1] The jury found the surgeon and hospital liable, and it apportioned 65% liability to the surgeon and 35% to the hospital. Upon appeal, the state's supreme court affirmed the judgment.

Several important issues arise from this case, which is consistent with the number of bases upon which the plaintiff alleged negligence. The first claim addressed by the court, and one of great importance to all physicians and healthcare facilities, was the lack of informed consent.

In general, physicians must fully inform their patients about the risks involved in any proposed procedure or treatment and possible alternatives to the procedure. Different jurisdictions might articulate the rule slightly differently, but the overall theme is the same: Physicians who fail to disclose important information to patients who are deciding about procedures might be found negligent for that failure.

THE COURT FOUND HERE THAT THE FAILURE TO INFORM ABOUT ALTERNATIVES AND THE SURGEON'S RELATIONSHIP WITH THE MANUFACTURER WERE RELEVANT.

In this case, Delaware had a statute defining "informed consent" that required the healthcare provider to give the patient a "reasonably comprehensible to general lay understanding" of information regarding the nature and risks, as well as alternatives, of the treatment that a reasonable patient would consider "material" to the decision. This provision of course leaves room for debate regarding whether something is "material," but physicians and hospitals can err on the side of caution and prevent any debate by informing patients in the first place.

The court here found that the failure to inform about alternatives and the surgeon's relationship with the manufacturer were relevant. The court found that this information was particularly relevant because, since the surgeon was earning money from the On-Q procedure, he had a "strong incentive to play down the risks of the On-Q procedure and play up the problems with alternative treatments." This law does not preclude physicians and facilities from having a financial interest in treatments or procedures, but if such is the case, patients must be informed of this fact to satisfy informed consent.

Physicians can be seduced by private companies to use their product or drug on patients without ensuring that these are FDA-approved to treat the issue at hand or that, if not, the medical staff and/or pharmacy leaders have approved the off-label use. Any time a product or drug is used in a study, regardless of by whom, the facility or regional institutional review board (IRB) has absolute oversight.

A physician or principal investigator might ask for an expedited approval from the IRB, but it should not be approved if it involves a device or drug not FDA-approved for use on a patient. Hospital IRBs should not be pressured by physicians to push through expedited approvals. Finally, any patient or subject participating must be asked to sign an IRB-approved informed consent form, which by law requires that all elements of informed consent be present along with additional elements related to being part of a research study. This process is above and beyond the usual informed consent a patient is given for more

routine procedures, and it can go a long way toward protecting physicians and healthcare facilities involved in disputes regarding informed consent should the issue arise later. Without going through appropriate research study protocols, there exists the possibility of kickback law violations as well.

Another important issue raised by this case is the different treatment that expert witnesses and fact witnesses receive by courts. Expert witnesses play an extremely important role for plaintiffs and defense in medical malpractice cases, as the knowledge required is typically beyond that which a layperson knows. Such scientific, technical, or otherwise specialized knowledge may be presented only by expert witnesses who have been qualified as such by the court prior to giving their expert opinion.

This qualification process can be quite involved and can include days of hearings to determine the expert's qualifications and reliability, so the complete scope goes beyond the purview of this article. However, of importance here is the fact that the trial court did not allow the defense's "fact witnesses" to opine on the fact that the procedure was "experimental" in nature, while it allowed the plaintiff's expert witnesses to testify about this fact as they possessed "specialized knowledge about what treatments for rib fracture pain generally were accepted in the medical community and what treatments were not." Choosing experts thus plays a critical role in litigation because if the court finds your "experts" are not properly qualified, this decision can be a death knell for your case without the experts' required testimony regarding medical subject matters.

REFERENCE

1. Supreme Court of Delaware, DE. Case No. N11C-06-092 MJB. Aug. 7, 2014. ■

Millions wasted in unused medical supplies and documented in U.S. ORs each year

Surgeons urge salvage of supplies to improve care in developing countries

A Johns Hopkins research team reports that major hospitals across the United States collectively throw away at least $15 million a year in unused operating room surgical supplies that could be salvaged and used to ease critical shortages, improve surgical care, and boost public health in developing countries.

A report on the research, published online Oct. 16 in the *World Journal of Surgery*, highlights not only an opportunity for U.S. hospitals to help relieve the global burden of surgically treatable diseases, but also a means of reducing the cost and environmental impact of medical waste disposal at home.

The fact of surgical supply waste is nothing new, the researchers note, but they say their investigation might be one of the first systematic attempts to measure the national extent of the problem, the potential cost savings, and the impact on patients' lives. While several organizations run donation programs for leftover operating room materials, such efforts would be far more successful if they were made standard protocol across all major surgical centers, the authors say.

"Perfectly good, entirely sterile and, above all, much-needed surgical supplies are routinely discarded in American operating rooms," says lead investigator **Richard Redett**, MD, a pediatric plastic and reconstructive surgeon at the Johns Hopkins Children's Center in Baltimore. "We hope the results of our study will be a wakeup call for hospitals and surgeons across the country to rectify this wasteful practice by developing systems that collect and ship unused materials to places that desperately need them."

The investigators based their estimates on an existing program that recovers and delivers unused surgical supplies from The Johns Hopkins Hospital in Baltimore to two surgical centers in Ecuador. The authors tracked 19 high-demand surgical items donated to the Ecuadorian hospitals over three years, then extrapolated the amount and value of the donations to 232 U.S. hospitals with caseloads similar to that of The Johns Hopkins Hospital. The results showed that if the 232 hospitals saved and donated unused surgical supplies, they would generate 2 million pounds of materials worth at least $15 million over a single year. Going a step further, the researchers tracked outcomes among 33 Ecuadorian patients whose surgeries were made possible as a result of the donations.

Their analysis showed that donated surgical supplies prevented, on average, eight years of disability per patient.

In the study, materials topping the 19-item surgical supplies list included gauze, disposable syringes, sutures, and surgical towels. However, the investigators say, it is important to tailor shipping to the specific needs of each hospital. Matching of donor leftovers to recipient need, they say, will prevent unnecessary shipping costs and avoid creating medical waste locally. In addition, the receiving hospital must have a demonstrated capability and the equipment to clean and sterilize the shipped materials before use in the operating room.

"Saving and shipping these materials is truly a low-hanging fruit enterprise, a simple strategy that could have a dramatic impact on surgical outcomes and public health in resource-poor settings and truly change people's lives," says Redett, who has been running the Johns Hopkins donation program since 2003. The Johns Hopkins initiative, known as Supporting Hospitals Abroad with Resources and Equipment (SHARE), was modeled after a similar program at Yale. ■

SDS Manager

Adding a surgery facility that is out of network

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

Is your surgery center locked into a bad contract with your payers? It happens.

You are so anxious to get your surgery center up and running and getting some cash flowing that, unfortunately, you grab at any payer contract, regardless of how bad it is. Most facilities typically live with poor payer contracts. This situation is true not just for surgery centers, but for hospitals as well!

Do you have no opportunity to attract new investor/user surgeons to your facility because no one wants to sell down their ownership?

Are you missing out on out-of-network reimbursement because you already are under contract with payers?

Have your surgeons asked you if you can keep patients longer than Medicare allows in the surgery center?

Are you one of the thousands of freestanding surgery centers that are in this situation?

But what if you develop another facility: a different center that allows you a new start, but still allows you to continue to operate the original facility? What if you have a new facility with no contracts with any payers and a different Medicare provider number? What if that new facility's leaders decide to stay out of network with payers until they get a contract they can live with that fairly compensates you for your hard work and investment?

You can.

There are some issues that need to be dealt with. Clearly some obstacles might lead you to believe it cannot be done, but it can. Here is just one example: A marginally successful freestanding surgery center is plugging along, doing about 300 multispecialty cases per month. The investor pool is roughly 70% surgeons and an outside investor group. The partnership has a non-complete clause with the surgeon investors. Pretty standard stuff.

The group would like to start doing spine procedures and more intensive orthopedic procedures and joint replacement that it currently cannot do at the existing facility due to several issues:

- Equipment is too expensive.
- There is a need for keeping patients beyond the 23-hour rule.
- Many of these new procedures are not on the Medicare approval list.
- There is poor or no reimbursement for these procedures.
- There is no room for the new investor surgeons in the current partnership, as no one wants to sell their shares.

What did we do?

1. Formed a completely new partnership, with some investors from the existing facility who want to do more intensive procedures.
2. Amended the original partnership agreement.
3. Established a new investor group with some members from the

COMING IN FUTURE MONTHS

- Getting your OR team to be more efficient
- Prevent delirium in your geriatric patients
- Best apps for outpatient surgery
- How to improve surgery collections

original, but mostly new.

4. Formed a new entity.

5. Established the new surgery center.

6. Obtained a new Medicare provider number.

7. Developed a recovery facility where patients might recover up to 72 hours.

This new facility has no payer contracts and stays out of network for its non-federal patients. Current investors from the original facility can perform their cases in either facility, depending upon the type of procedures and whether their patients need to stay overnight or longer.

What is the opportunity for a hospital in this scenario? Clearly hospital leaders also are seeing their surgical reimbursement margins deteriorate. They know they are going to continue to lose their high value surgical volume to surgery centers. Their ability to partner with this next generation of surgery centers will help them maintain part of their eroding profits. *[Earnhart & Associates is a consulting firm specializing in all aspects of outpatient surgery. Earnhart & Associates' address is 5114 Balcones Woods Drive, Suite 307-203, Austin, TX. 78759. Phone: (512) 297.7575. Fax: (512) 233.2979. E-mail: searnhart@earnhart.com. Web: www.earnhart.com.]* ■

ASC Association takes issue with new PA report

The average revenue per visit to an ambulatory surgery center (ASC) in Pennsylvania rose 4.8% to $1,084 between Fiscal Year (FY) 2012 and FY 2013, according to a new analysis from the Pennsylvania Health Care Cost Containment Council (PHC4) in Harrisburg.

The Ambulatory Surgery Center Association (ASCA) was quick to respond to the *2013 Financial Analysis: Volume Two: Ambulatory Surgery Centers* report. "While the PHC4 report contains some interesting data about Pennsylvania ASCs, it falls short of presenting an accurate profile of the real-life operating value that ASCs provide to their patients and the state of Pennsylvania," the ASCA said. "In addition, as the authors of the report point out, the data must be considered carefully before any conclusions can be drawn."

ASCA released a statement that included the following points:

• In 2012, Medicare saved more than $39 million because of the program's beneficiaries in Pennsylvania who elected to have their cataract surgery performed in an ASC. On just 2,900 arthroscopic knee and shoulder surgeries performed in Pennsylvania ASCs, Medicare saved more than $2.6 million. Pennsylvania patients saved $5.8 million on colonoscopies because they were performed in ASCs. Nationally, these savings translate into $2.6 billion per year in savings for Medicare and its beneficiaries.

• The ASC community is committed to quality, and in the first full year of Medicare's national ASC Quality Reporting Program, 98.8% of Pennsylvania ASCs successfully met the program's reporting requirements.

• Two-thirds of ASCs nationwide provide free or reduced cost care for patients and receive no financial incentives for providing that care.

• Finally, while some of the financial data the report contains references ASC margins, it is important to recognize, as the report indicates, that those numbers do not account for two important factors that would reduce those margins significantly: taxes paid and disbursements to physicians, which they receive instead of a salary.

"Because of the high quality, lower cost care that ASCs provide, they continue to gain popularity among patients," the ASCA said. "As the fight to contain health care costs continues, ASCs represent a substantial value and a model of success."

PHC4 is an independent state agency that reports information that can be used to improve the quality and restrain the cost of healthcare in Pennsylvania. Copies of *Financial Analysis 2013, Volume Two* are free and available at http://www.phc4.org. ■

Life Safety Code surveyor added

Since Dec.15, 2014, The Joint Commission has added a Life Safety Code (LSC) surveyor to the survey team for ambulatory surgical centers (ASCs).

The LSC surveyor will conduct survey activities with the clinical surveyor.

The change applies to ASCs that do the following:

• select the Medicare deemed status option;

• seek ambulatory healthcare accreditation and are classified as an ambulatory healthcare occupancy (excludes business occupancy).

The Joint Commission Connect extranet site includes the agenda for the LSC surveyor's activities in the "Survey Activity Guide." ■

SAME-DAY SURGERY

CNE 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 until Jan. 4, log on to cmecity.com to take a post-test. First-time users must register on the site using the 8-digit subscriber number printed on your mailing label, invoice, or renewal notice. On and after Jan. 5, when logging onto the new AHCMedia.com site, go to "MyAHC" and then "My Courses" to view your available CE activities.

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

4. After successfully completing the test, your browser will be automatically directed to the activity evaluation form.

5. Once the completed evaluation is received, a credit letter will be e-mailed to you.

CNE QUESTIONS

1. According to a recent report from IS Decisions, what percent of former employees go into their former employer's information systems?

A. Nearly one in 100
B. Nearly one in 50
C. Nearly one in 20
D. Nearly one in 10

2. The FBI recently warned healthcare industry companies that they are being targeted by whom?

A. Hackers
B. Domestic terrorists
C. International terrorists

3. What changes did an Illinois hospital make after duodenoscopes had bacterial contamination associated with an outbreak of a highly resistant strain of *E. coli*?

A. Changed its policies and procedures on outbreaks.
B. Changed its duodenoscope reprocessing to gas sterilization
C. Changed qualifications for its reprocessing staff

4. In the case involving the On-Q procedure, which of the following happened?

A. The patient was not given the choice of having epidural anesthesia.
B. The surgeon failed to disclose his own personal financial interest in the procedure.
C. Both A and B
D. Neither A nor B

CNE OBJECTIVES

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

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

GOLF SURGICAL CENTER

INFECTION CONTROL BREACH REPORTING POLICY and PROCEDURES

POLICY: It is the policy of this facility prevent, control, investigate and, as required, report to State public health authorities certain breaches in recognized infection control practices.

BACKGROUND: Medicare regulationsrequire adherence to generally recognized standards for infection control practices. The Medicare Standards at 42 CFR §416.51 for ambulatory surgical centers (ASCs) states, "The ASC must maintain an infection control program that seeks to minimize infections and communicable diseases....(b)...The ASC must maintain an ongoing program designed to prevent, control, and investigate infections and communicable diseases. In addition, the infection control and prevention program must include documentation that the ASC has considered, selected, and implemented nationally recognized infection control guidelines...."

Some types of infection control breaches, including somespecific to medication administration practices, pose a risk of bloodborne pathogen transmission that warrant engagement and involvement of public health authorities to conduct risk assessment and, if necessary, to implement the process of patient notification.

PROCEDURE: **Breaches to Be Referred to State public health authorities**

When one or more of the following infection control breaches is identified at this Medicare- and/or Medicaid-certified ambulatory surgery center, efforts should be madeby this ASC to make the appropriate State public health authority aware of the issue and to ask them to address and, if warranted, to investigate the potential risk:

•Using the same needle for more than one individual (always follow the "One Needle / One Patient / One Time" practice);

•Using the same (pre-filled/manufactured/insulin or any other) syringe, pen or injection device for more than one individual (always follow the "One Needle / One Patient / One Time" practice);

•Re-using a needle or syringewhichhas already been used to administer medication to an individualto subsequently enter a medication container (e.g., vial, bag), and then using contents from that medication container for another individual(always follow the "One Needle / One Patient / One Time" practice); and/or

•Using the same lancing/fingerstick device for more than one individual, even if the lancet is changed (always use disposable lancing devices or sampling from a blood draw/IV start).

Otherinfection control breaches in addition to those described above, if recommended or required by State public health authorities or believed to require public health assessment and management, will be reported by this ASC to State public health authorities.

Thespecificactions of reporting, assessing and managing potential risks and the possible need to notify patients fall outside the jurisdiction of the Centers for Medicare & Medicaid Services (CMS), but do fall within the authority of State public health agencies.

Reporting to the State public health authority will be initiated by the Infection Control Officer (a qualified RN) in consultation with both the Director of Nursing and the Medical Director and a copy of the report presented as a part of this facility's Infection Control Program.

Reporting contact:

•Division of Patient Safety and Quality
Illinois Department of Public Health
122 S. Michigan Avenue 7th Floor, Chicago, IL 60603

2014 Contact information:

DIVISION OF PATIENT AND SAFETY QUALITY	DRISCOLL, MARY	122 S. MICHIGAN AVE. , 7 CHICAGO 60603	312-793-2051

SAME-DAY SURGERY

How do you successfully manage employees ranging from Millennials to Baby Boomers?

By **Joy Daughtery Dickinson**, Executive Editor

As an outpatient surgery manager, you might be managing employees from four generations. Older staff aren't retiring quickly, so you might be managing employees who are older than you. How do you do all of this successfully?

"Because each group has different characteristics and values, healthcare providers need to educate and create an awareness around the diversity of each group as well as their similarities," says **Donna J. Doyle**, MS, RN, CNOR, NE-BC, administrative director of surgery and anesthesia at Grant Medical Center in Columbus, OH. "This awareness needs to occur with staff as well in order to foster an environment of respect for each individual."

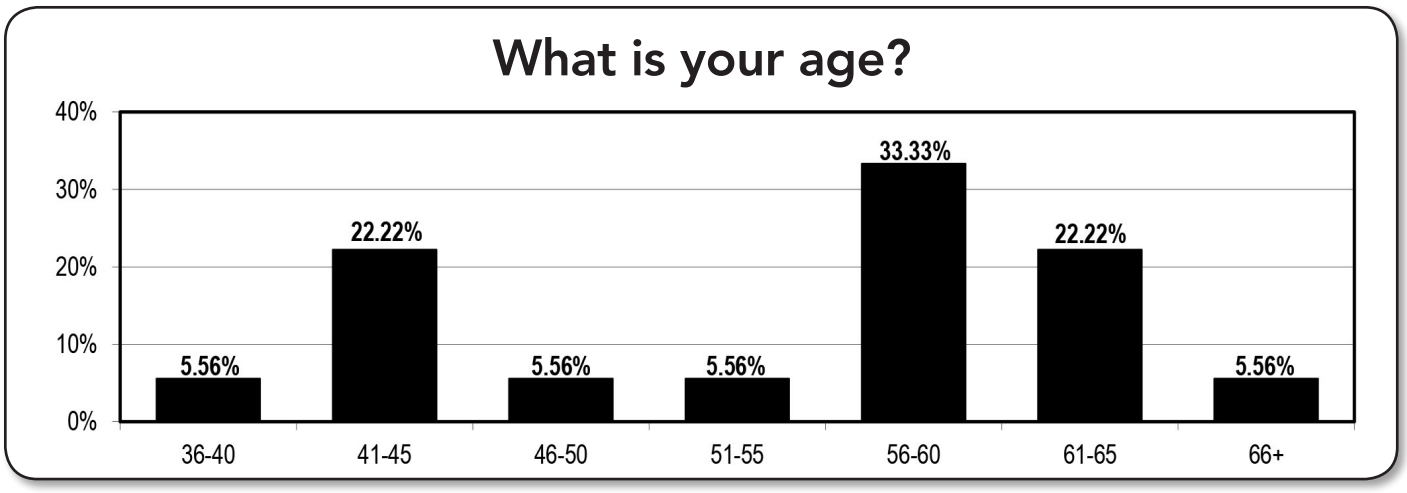
Having this type of environment will help attract staff members of all ages, Doyle says. "Our patients come from all generations, and we need a workforce that will be able to acknowledge and understand the diversity of our patient and workforce populations," she says.

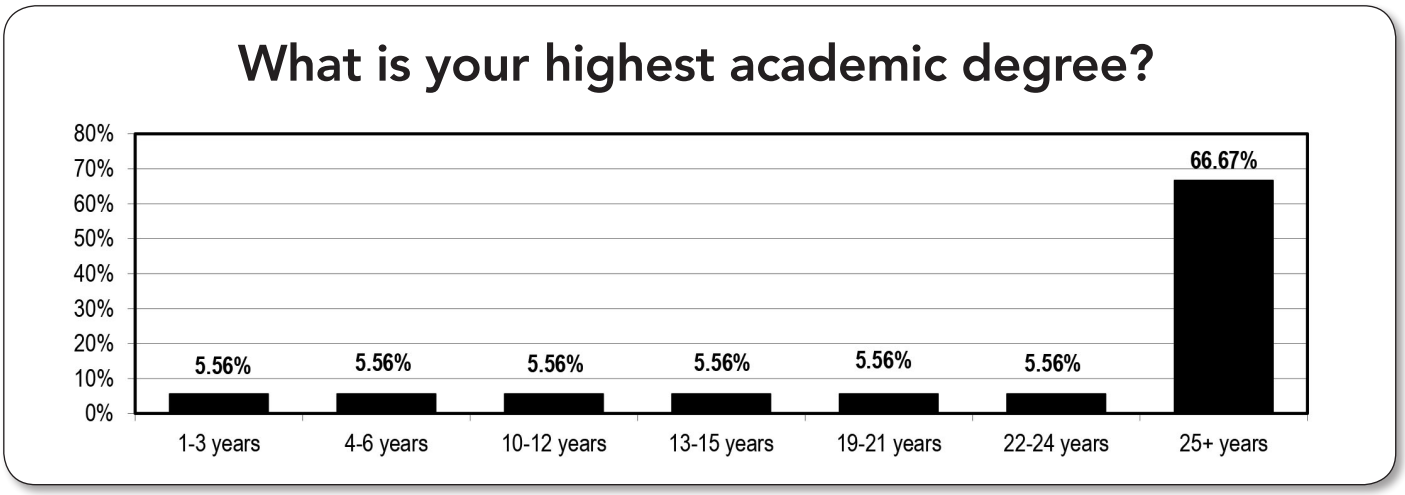
The variety of ages is clear from the results of the *Same-Day Surgery 2014 Salary Survey. (See graphic, below.)* Consider these suggestions for managing multiple generations:

• Understand what different generations value.

For teaching millennial employees, the best approach is "learning with," says **Chip Espinoza,** PhD, co-author of *Managing the Millennials: Discover the Core Competencies for Managing Today's Workforce* and academic director for organizational psychology at Concordia University, Irvine (CA).

With mentoring, the dynamic should approach that of a friend/supporter, Espinoza advises. "You can set up situation where they are discovering together,"





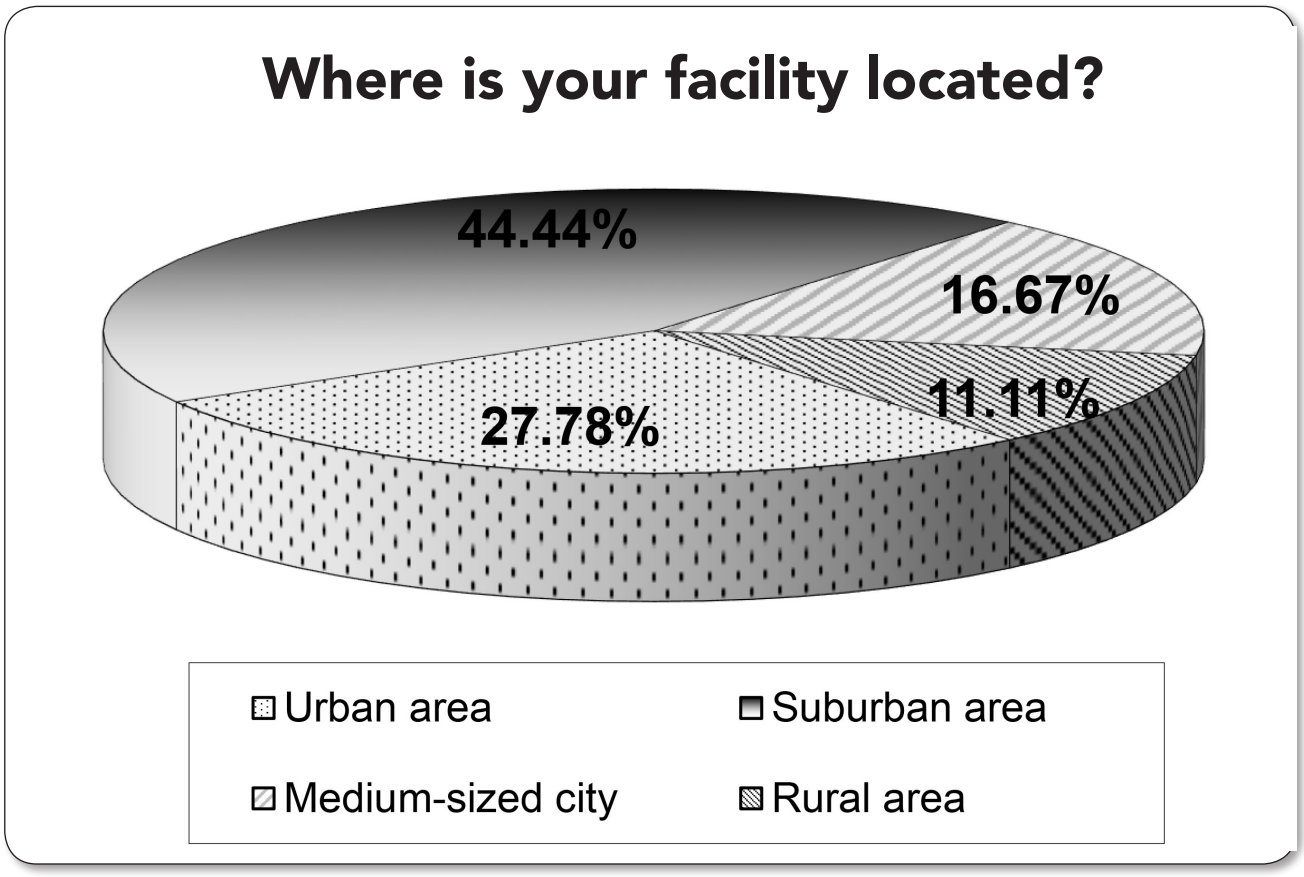
he says. Keep in mind that this generation is the first one that hasn't needed an authority figure to access information, because with mobile devices, they always have access to information. Harness that ability by having employees bring in information and share with the rest of the staff, urges says **Dianne Appleby**, RN, BSM, MBA, executive director/administrator at Menomonee Falls (WI) Ambulatory Surgery Center. Her facility has a retention rate that stays at about 98-99%.

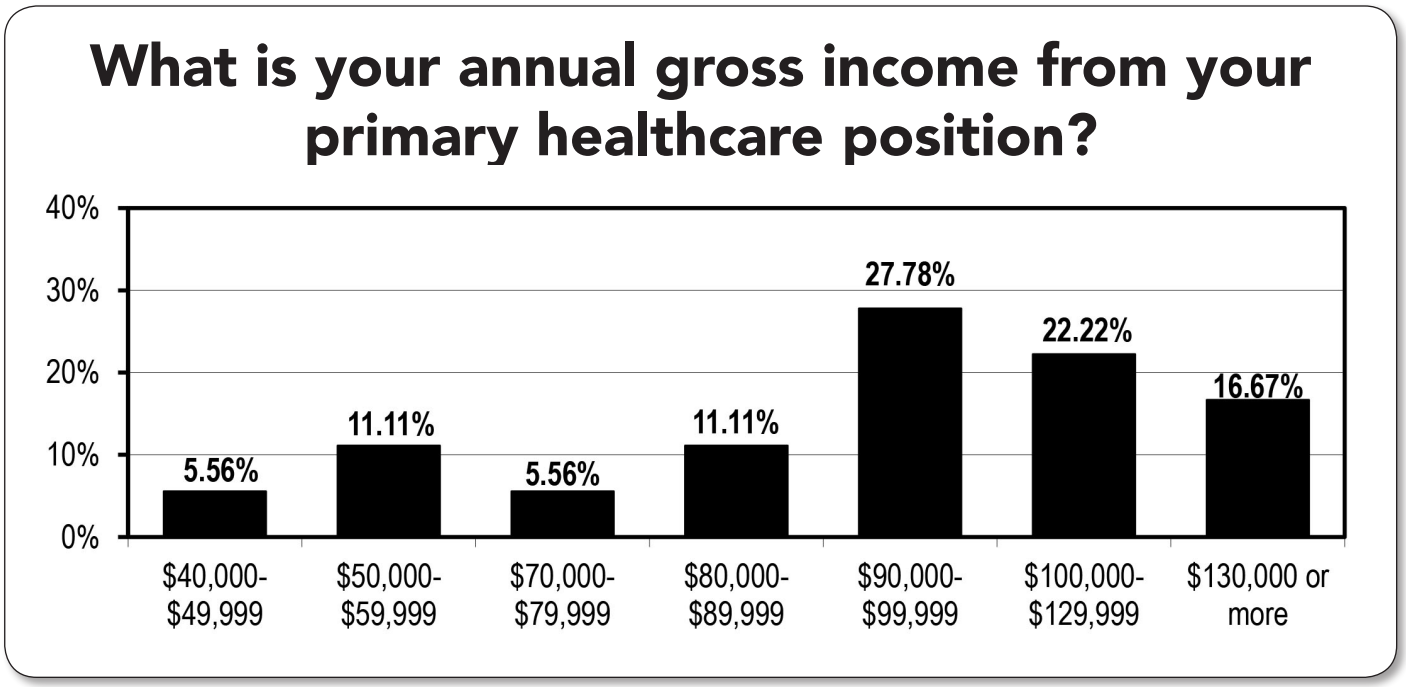
"When you empower people to go out and get information, bring it in, and put it into practice, anyone appreciates that personal growth, not just millennials," Appleby says. "That is something we encourage everyone to do."

Younger employees are very comfortable with technology and multitasking, and they value flexibility, Doyle says.

Menomonee Falls offers flex hours, Appleby says. "They stay, when they're getting close to retirement, because they enjoy the flexibility of hours and environment, so they don't leave," she says. *(Salary survey results show that 66.7% of respondents have worked in healthcare for 25 plus years. See graphic, above.)*

Millennials also need flexibility in work/life blending, Espinoza says. "They don't mind accessing their work life in their personal time, but





they want to access their personal life in work time," he says. "They don't see a fine line between work and life as much as previous generations would." This need for flexibility should be considered in your Internet policies, Espinoza advises.

• Create a culture that allows employees to work independently and gives them opportunities to grow.

Appleby attributes her strong retention rate in part to her facility's culture. "We respect people's experience, their knowledge, and we give them the latitude to work autonomously so they're empowered to use that skill and knowledge," she says.

Instead of being micromanaged, employees are given the opportunity to help develop policies and educational opportunities. "Anytime you have an organization where people feel ownership, and they have ability to help determine, self-determine, what their role will be, with that freedom, people want to stick around," Appleby says.

Doyle says younger employees are comfortable working in teams but want to contribute individually. "Harness this to move your teams forward," she suggests.

Millennials want to be taken seriously by having a voice in the running of their facility, Espinoza agrees. Allow them to participate in brainstorming and problem-solving, he says. They look for simpler ways of doing tasks, so be flexible, he urges. If they think they have nothing to contribute from a problem-solving or creativity standpoint, that's a turnoff, he says.

At the same time, however, millennial employees realize they lack experience, and they want opportunities to grow, such as cross training, Espinoza says. They need to know that authority figures are there to help them achieve their goals, he says.

At Menomonee Falls, if techs want to work in a different area or want to be certified, they are given the opportunity to move around or learn new skills. Their salaries also help to keep them working at the surgery center, Appleby says. "We had to look at our competition," she says. "Our techs get paid very well, comparable to hospitals, and the benefit package is a good one. Couple that with the hours, and they don't leave us."

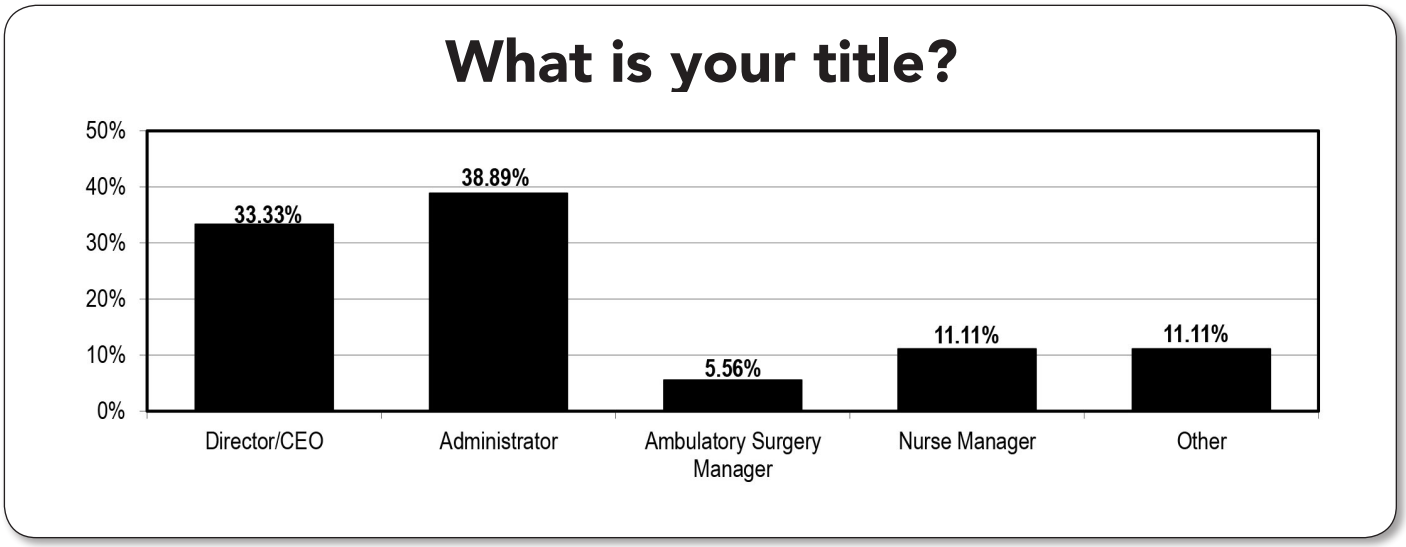
Older leaders might have different priorities. Montefiore Medical Center in New York City has been recognized by The New York Academy of Medicine (NYAM) in New York City as an inaugural Age Smart Employer Award winner. Montefiore was awarded for its recruitment, retention, and development practices as well as its investment in late career employees.

Programs include a Leadership Development Academy offering seasoned leaders the opportunity to advance their skills in education courses, formalized mentoring, coaching partnerships, and career counseling workshops. A 25 Year Club recognizes those with 25 years of service. Inductees are members for life and meet annually with executive leadership for a celebration. The 25 Year Club has more than 3,000 members. When Montefiore associates retire, they are offered the opportunity to join a special volunteer network.

• Give them clear rewards.

With younger employees, the more clear you are about the rewards, the better off you'll be, Espinoza says. "Assumptions are made by management or organizations about how things have always been done, but this group doesn't understand that," he says.

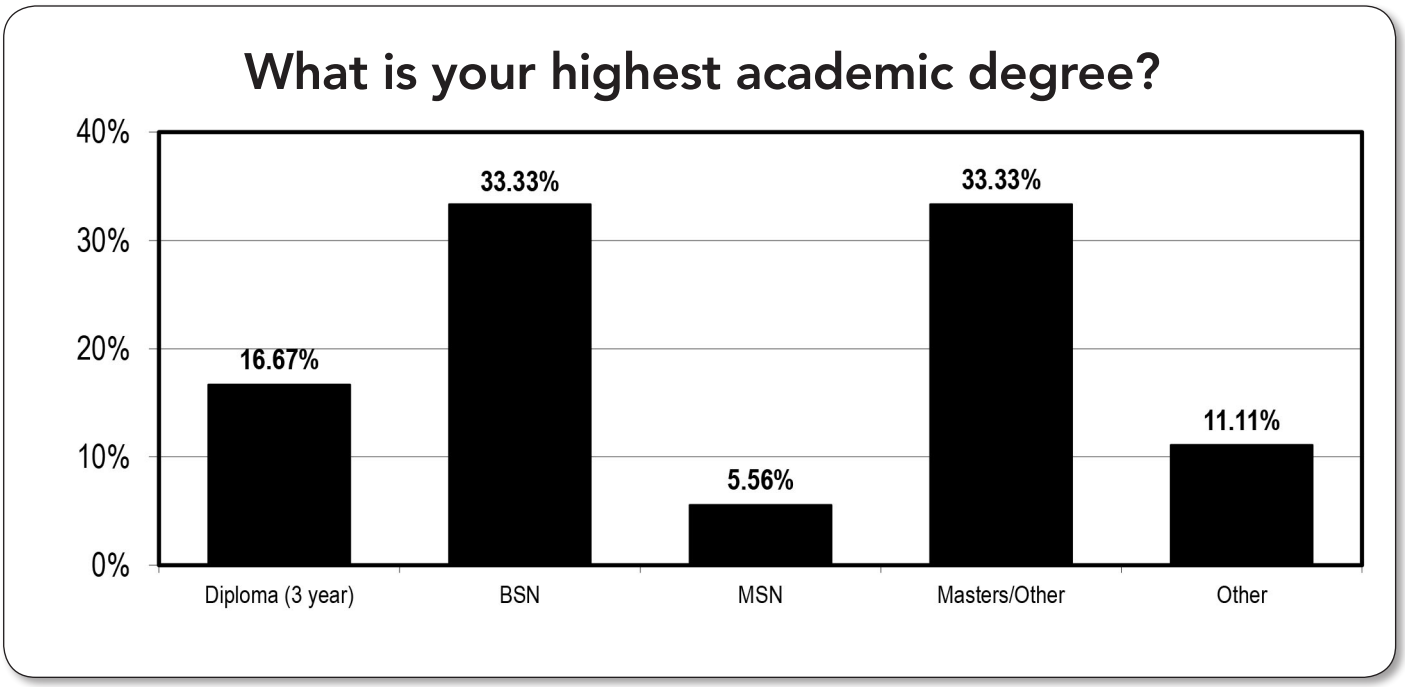
Millennials lack patience and want



to be promoted faster, Espinoza says. Keep them engaged in conversations about their development, he says. "They may feel stalled because they don't understand how important what they're doing is to their future," Espinoza says.

Provide feedback on their progress, and be clear, he says. "This group's kryptonite is ambiguity," Espinoza says. "They like things detailed and spelled out, because that's what they're looking for."

Attracting younger employees is critical, because they have multiple career choices available to them today, Doyle says. Additionally, as the average age of perioperative nurses rises, outpatient surgery providers face a "profound nursing shortage," she says. "So we need to use every tool at our disposal to combat this shortage. Knowledge is power, and knowledge of generational differences that we can use in recruiting and retaining staff will make a difference in being able to maintain OR access for our patients." *(Editor's note: The* Same-Day Surgery Salary Survey *was mailed in the September 2014 issue to 160 subscribers and had 18 responses, for a response rate of 11%.)* ■



Dear *Same-Day Surgery* Subscriber:

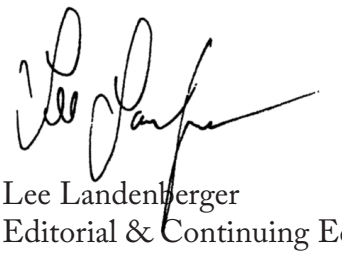
Here's a change we know you'll like: From now on, you can earn continuing education credit for each individual issue. No more having to wait until the end of a six-month semester or calendar year to earn your continuing education credits or to receive your credit letter.

Starting now, you can earn up to
• 1.75 AMA PRA Category 1 Credits™ for each issue and up to 21 annually.
• 1.37 nursing contact hours for each issue and up to 16.4 total annually.

Here's how to earn your credits:
1. Read and study the activity, using the provided references for further research.
2. Log on to cmecity.com to take a post-test. First-time users must register on the site using the 8-digit subscriber number printed on your mailing label, invoice or renewal notice. After Jan. 5, 2015, log onto AHCMedia.com and click on MyAHC.
3. Pass the post-test with a score of 100%; you will be allowed to answer the questions as many times as needed to pass.
4. Complete and submit an evaluation form.
5. Once the evaluation is received, a credit letter is emailed to you instantly.

If you have any questions about the process, please call us at (800) 688-2421 or outside the United States at (404) 262-5476. Our fax is (800) 284-3291 or outside the United States at (404) 262-5560. We are also available at customerservice@ahcmedia.com. Thank you for your trust.

Sincerely,



Lee Landenberger
Editorial & Continuing Education Director