# Same-Day Surgery®

35th Anniversary

Covering Hospitals, Surgery Centers, and Offices for More than 35 Years

**July 2012:** Vol. 36, No. 7
Pages 69-80


## IN THIS ISSUE




**Financial Disclosure:**
Executive Editor **Joy Dickinson**, Board Member and Nurse Planner **Kay Ball**, 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. **Mark Mayo**, Consulting Editor, reports that he is director of ambulatory services, Ambulatory Surgical Care Facility, Aurora, IL. **Steven Schwaitzberg**, MD, Physician Reviewer, discloses that he is on the speakers bureau for Stryker Corp. and Merck & Co., he is a medical advisor to Surgiquest, and he is a stockholder in Starion Instruments.


# Breach of outpatient surgery records raises red flag — Know and protect your data

Cyber attacks. Data thefts. System breaches. They're all on the rise, and healthcare is the no. 1 field at risk, according to a just-released Internet Security Threat Report — 2011 Trends from Symantec Corp.[1] Consider these recent examples from the outpatient surgery field:

• Earlier in 2012, St. Elizabeth's Medical Center in Boston notified almost 7,000 patients that their billing information, including credit card numbers and security codes, might have been compromised.[2] The documents were removed by a vendor from a building that was about to be demolished and were to be shredded. A few days later, an individual reported finding cashier's receipts for credit card payments made by five patients, including some from the hospital's surgery center, blowing through a field in another neighborhood. The receipts included patients' names, hospital account numbers, credit card numbers, security codes, and expiration dates.

• Also earlier this year, Emory Healthcare in Atlanta found that 10 backup discs containing information on surgical patients were missing from a storage location at one of its hospitals. The information on the discs was from about 315,000 surgical patients treated at one surgery center and two of its hospitals. The discs contained patient names, dates of surgery, diagnoses, procedure codes or the name of the surgical procedures, device implant information, surgeons' names, and anesthesiologists' names. About 228,000 of the patient records included Social Security numbers. All affected patients were provided identity protection services, including credit monitoring, and access to a toll-free hotline for questions. Any patient who discovers identity theft or fraud issues within one year is provided an investigator to

## This Month: Our best tips for how not to get sued

This month is one of the most anticipated issues of the year for *Same-Day Surgery* readers: Our special focus on liability in outpatient surgery. We tell you about three facilities that recently had data breaches involving outpatient surgery records, and we give you multiple tips to avoid getting into the same situation. We also tell you specifically how a facility reduced the number of incorrect counts and count discrepancies by half. This issue also gives you the legal specifics of a retained sponge case and explains who was liable. We also give you some new guidelines on using background checks with employee applicants. Enjoy this special issue! ■




AHC Media

help them restore their identity. *(For more information, view Emory Healthcare's "Notice to Our Patients" at www.emoryhealthcare.org/protection.)*

Emory leaders acknowledge that the discs had not been stored according to the facility's protocol, according to a published report.[3] The discs were in an office cabinet that was not locked at night, although it was on a restricted hallway, the media report said. The information on the discs was associated with an outdated system and, thus, was not encrypted. Additionally, in 2011, bills of 32 patients at Emory's orthopedic clinic were stolen, and information was used to file fraudulent tax returns in the names of nine of those patients, the media report said.

Stolen patient data can put an outpatient surgery program into legal problems fast. "In addition to HIPAA, there are several states that have pertinent laws, says **Joe Santangelo**, MS, principal consultant at New York City-based Axis Technology, which provides data security services.

## What would it cost you? Maybe millions

And then there's the cost. Emory estimates that this latest incident cost the healthcare system between $1.5 and $2 million. There were no fines.

"If you are found to have a breach, it can be a very costly and potentially debilitating affair," Santangelo says. He points to a recent example of a small surgery center with 5 physicians that was fined $100,000 by the Office of Civil Rights (OCR) for failing to protect patient information.[4] "The investigation found that the practice failed to implement adequate policies and procedures to protect patient information, did not document that it provided HIPAA training to employees, failed to conduct risk analysis, and failed to obtain proper agreements from business associates," Santangelo says. *(To see the resolution agreement, go to http://1.usa.gov/IlVjXX.)*

He points out that in addition to the costs of notifying patients, investigating and controlling the breach, and potential litigation and fines, there are intangible costs such as damage to your brand, loss of customers, decline in practice value, and reputation management. "Thus providing proper security of patient information is actually a cost-effective practice, when looked at in terms of the cost of a breach," Santangelo says.

Healthcare is vulnerable 24/7, says **Anne Adams**,

## EXECUTIVE SUMMARY

Two incidents involving outpatient surgery records earlier this year have brought the dangers of data breaches to the forefront of managers' priorities.

- Determine what vulnerable patient or employee information you have in paper or disc format.
- Reinforce and clarify existing policies and procedures for safeguarding the security and privacy of sensitive information. Make sure staff members understand the definition of "secure."
- Consider a checklist of data-related items to discuss with new employees.
- Be transparent when communicating with patients and staff.
- Have a process for destruction of documents that is clear and workable. Have clean desk policies and clearly marked locked bins to house documents to be shredded.

**Same-Day Surgery**® (ISSN 0190-5066) is published monthly by AHC Media, a division of Thompson Media Group LLC, 3525 Piedmont Road, NE, Building Six, Suite 400, Atlanta, GA 30305. Telephone: (404) 262-7436. Periodicals Postage Paid at Atlanta, GA 30304 and at additional mailing offices.

**POSTMASTER:** Send address changes to Same-Day Surgery®, P.O. Box 105109, Atlanta, GA 30348.

SUBSCRIBER INFORMATION

Customer Service: (800) 688-2421 or fax (800) 284-3291, (customerservice@ahcmedia.com). Hours of operation: 8:30 a.m. to 6 p.m. Monday-Thursday; 8:30 a.m.-4:30 p.m. Friday.

Subscription rates: U.S.A., one year (12 issues), $499. Add $17.95 for shipping & handling. Outside U.S.A., add $30 per year, total prepaid in U.S. funds. Discounts are available for group subscriptions, multiple copies, site-licenses or electronic distribution. For pricing information, 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.)



AHC Media 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 16.5 nursing contact hours using a 60-minute contact hour.

Provider approved by the California Board of Registered Nursing, Provider #14749, for 16.5 Contact Hours.

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

AHC Media designates this enduring material for a maximum of 20 *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** (229) 551-9195 (joy.dickinson@ahcmedia.com).
Production Editor: **Kristen Ramsey**.
Senior Vice President/Group Publisher: **Donald R. Johnston**.



AHC Media

Editorial Questions
Questions or comments? Call Joy Daughtery Dickinson at (229) 551-9195.

chief privacy officer at Emory Healthcare. Adams spoke openly with *Same-Day Surgery* about the privacy breach and shared a presentation on the incident that she gave earlier this year to the University Risk Management and Insurance Association (URMIA) Southeastern Regional Conference.[5]

Some of the reasons for healthcare's vulnerability? Data is used across multiple locations, and you have a vulnerable population that includes patients under anesthetics. In addition, medical facilities have substantial traffic, says **Arthur J. Fried**, JD, member of Epstein Becker Green in New York City.

**Neil Roiter**, research director at Corero Network Security in Hudson, MA, says, "With the reported rise in data breaches in the healthcare sector, it is imperative that patient information is secure in any environment: an outpatient surgery center, hospital, or doctor's office. Data protection policies, procedures, and security technologies for outpatient surgery centers must be part of a holistic organizationwide security program." Corero Network Security is an international network security company and the leading provider of Distributed Denial of Service (DDoS) defense and Next Generation Intrusion Prevention System (IPS) solutions.

"High-profile healthcare record breaches … appear to show a pattern of lax standards regarding the handling of sensitive patient data and, in many cases, inadequate processes and procedures to ensure that data is not lost or stolen through carelessness by employees or partners," Roiter says.

Consider the lessons learned from this year's data breaches:

**• Know what data you have that is at risk.**

After the data breach, Emory conducted a comprehensive inventory of all physical spaces across the system to ensure data were properly secured. Adams said, "That is the real lesson learned: To make sure everyone is aware of what they have, in terms of patient information, whether it is electronic or paper, within their environment."

To protect your data, understand where personal health information (PHI) exists in your environment, Santangelo says. "The inventory should be sufficiently automated and audited periodically and needs to be updated as new functionality is introduced and new reports are introduced," he says. "Once we understand where the PHI exists, we can have a plan for safeguarding this data."

At Emory, the "net" of protected information has been broadened to include not just patient information, but employee information.

**• Ensure that employees and partners understand policies and procedures for handling patient information.**

Emory Healthcare launched an institutionwide initiative using inservices to reinforce and clarify existing policies and procedures for safeguarding the security and privacy of sensitive information.

In smaller facilities, use a checklist or set of procedures when new employees start, and review them periodically for updates in requirements and changes in procedures, Santangelo advises. They should be easily accessible to pertinent staff, he says. The checklist should include items such as:

– administration of confidentiality statements;
– providing copies of requested medical record;
– secure filing and maintenance of documents;
– procedures for secure destruction of documents;
– inventorying and managing technology assets;
– utilization of social media. *(For more information on social media, see p. 77. Also see these stories in* Same-Day Surgery*: "All it takes is a few keystrokes, and your facility's reputation is ruined," April 2012, p. 37, and "Patient info on Facebook traced to temp staff," May 2012, p. 54.)*

**• Work to regain patient trust.**

Part of your assessment of a data breach should be the impact on your reputation, Adams says. "That could be even more harm to the institution than a financial standpoint: losing patient trust," she says.

To address this concern, Emory promoted a policy of transparency in letters sent to patients that explained every aspect of the data breach. "We had to put it in a format that people would understand, and not get too much 'into the weeds," because that's what happens," Adams says.

Emory strived to reassure patients that the breach was an isolated situation. "We are revising our policy to ensure people understand 'secure,'" Adams says. "When I personally talk to patient, I would tell them that." *(For more information on internal communication, see story, p. 72.)*

In the end, securing your data is a win-win situation, Santangelo says.

"Providing security around patient data and restricting access to data is not only morally ethical and legally required, but is a sound business practice that has a real return on the investment made," he says. *(For information on how to secure access to sensitive information, see story, below.)*

## REFERENCES

1. Symantec Corp. Internet Security Threat Report — 2011 Trends, Volume 17. Published April 2012. Accessed at http://www.symantec.com/threatreport.
2. Weisman R. St. Elizabeth's Medical Center notifies patients of

billing data breach in Charlestown incident. *The Boston Globe*. April 6, 2012. Accessed at http://bo.st/HQMjtu.
3. Teegardin C. Patient data missing for 315,000 Emory patients. *The Atlanta Journal-Constitution*. April 18, 2012. Accessed at http://bit.ly/JcFRjJ.
4. Department of Health and Human Services Press Office. HHS settles case with Phoenix Cardiac Surgery for lack of HIPAA safeguards. April 17, 2012. Accessed at http://1.usa.gov/IUpWr7.
5. Adams A. Anatomy of a Breach: Effective Investigation, Analysis, and Mitigation Steps in Privacy Breaches. Presented to the University Risk Management and Insurance Association (URMIA) Southeastern Regional Conference, Feb.28, 2012.

**RESOURCE**

• Open Security Foundation maintains a database of data breaches. Web: http://datalossdb.org ■

# How to secure access to sensitive information

Physical security of your sensitive protected health information (PHI) is critical, says **Joe Santangelo**, MS, principal consultant at New York City-based Axis Technology, which provides data security services.

That step means "ensuring access to areas where PHI is handled by only those who must have access to that data," Santangelo says.

Have a process for destruction of documents that is clear and workable within your staff's working environment, he says. "Clean desk policies, as well as clearly marked locked bins to house documents to be shredded, are important," Santangelo says.

Assess your policies periodically, and document this self-assessment for regulators, he advises. "Any sensitive data that resides on devices should be encrypted," Santangelo. "In the event that the device falls into the wrong hands, this will provide security from less sophisticated threats and buy time from more sophisticated ones."

Use asset controls, including documentation of asset retirement or destruction, he says. "Ideally, mobile devices will have an on-device protection solution and be ready to be remotely disabled in the event that they are lost or stolen," Santangelo says.

Use a data loss protection (DLP) solution to oversee movement of data, he says. "This can range from standard network monitoring and PC protection software to very sophisticated suites which provide both intrusion detection and prevention," Santangelo says.

After a recent data breach, Emory Healthcare in Atlanta asked staff members to examine their area and record what information they have and where it is located, and then ensure the information is physically secure. "For example, maybe they have laptops that aren't encrypted, or data disks that aren't encrypted, or other such information," says **Anne Adams**, chief privacy officer at Emory Healthcare.

Staff members are asked to immediately secure the information, such as making sure it is in a locked file cabinet in a locked office. In the long term, Emory is looking at moving patient/employee information to a secure server, while purging paper files.

"We remind people: If you can purge it, do it," Adams says. Sensitive information is shredded and picked up by a vendor. "We're also ensuring any backup data is on an approved system server, or it has to be in an encrypted environment, which has to be approved," Adams says.

Involve your IT staff in security of electronic data, says **Mark Mayo**, executive director of the ASC Association of Illinois and director of ambulatory services at Ambulatory Surgical Care Facility, Aurora, IL. Under the Health Information Exchanges (HIE) federal program, several states are setting up secured electronic interface security systems for sending and sharing PHI. IT should be certain that thumb drivers or downloadable ports — discs or printouts — are disabled, Mayo says. "There needs to be IT review of data traffic to look for unauthorized access to data in areas when info is not needed," he says. "IT needs to make sure that data is encrypted and that firewalls are in place to detect and deter hackers." ■

# Internal communication is key during breach probe

Keep people in the loop. That's always good advice, but perhaps never more important than after a data breach.

That suggestion comes from **Anne Adams**, chief privacy officer at Emory Healthcare, which suffered a data breach earlier this year.

Tell your board members early when you have a breach so they're not caught off guard, Adams says. Otherwise, if your board members also are patients, they might receive a letter about the breach before they're notified as a board member, she warns.

Also, Emory ensures that staff members and physicians are informed of breaches. "We send out a communication, usually at the same time that letters are sent to patients or before it would appear in the media," Adams says. "This way, if staff receive calls from patients or if patients have concerns, staff can address it with the patient or know where the patient

can receive additional information." *(A copy of Emory's breach notification checklist is included with the online issue.)* ■

# Surgery staff reduces count problems by 50%

*Incorrect counts, discrepancies cut*

According to The Joint Commission, retained surgical items resulting in death or permanent loss of function were the most frequently reported sentinel event in 2010 and 2011.

Help is on the way from Boston Children's Hospital, which reduced the number of incorrect counts and count discrepancies by 50% between 2009 to 2010. Maintaining that success has proved challenging as the hospital has opened satellite facilities in the suburbs and taken on more sicker patients; however, the hospital reports no incorrect sponge counts for 2011.

The process started when **Cornelia Martin**, RN, CNOR, level III staff nurse in OR risk management, determined through incident reports that the OR was reporting a large number of count discrepancies. "According to the retained items literature, count discrepancies on their own can contribute to retained items," Martin says.

The hospital took these steps:

**• Standardize how counting is done.**

As staff reviewed the counting process, they determined they needed to standardize how counting was done every time, for every patient, in every procedure.

Staff determined that not only did they need standardization in how they counted, but also where they documented the counts, says **Elizabeth K. Norton**, BSN, RN, CNOR, level III staff nurse and main OR patient safety and quality nurse. "Some were doing it on the blackboard, some on a piece of paper, some on the back of a sheet, some on their pants leg, and some on the count sheet," Norton says.

**• Educate the staff.**

Boston Children has a mandatory policy that with any discrepancy in the count, an X-ray is taken.

Martin says, "We wanted to let nurses know that not only do count discrepancies increase the time spent in the OR looking for an item or to resolve a discrepancy, but it also causes patient to have an X-ray that costs about $500 per X-ray just to rule out retained needles or any other items. It causes patients to have unnecessary exposure, most importantly."

Staff were re-educated that if an X-ray was obtained, that was the end of the searching process. However, staff also were re-educated that X-rays don't always pick up retained items. "We want people to be very aware that an X-ray is not the `be all and end all,'" Martin says. *[A copy of their revised count policy is enclosed with the online issue of* Same-Day Surgery. *For assistance, contact customer service at (800) 688-2421 or customerservice@ahcmedia.com.]*

**• Minimize distractions.**

Boston Children's determined that distractions could be a contributing factor to count discrepancies. Norton says, "We had to make sure surgeons were all on board that when we're counting, we can't be interrupted. No distractions mean no answering pages during the counting process and turning down the music," she says, so the count can be done "efficiently and accurately without distraction and interruption."

**• Consider technology.**

In 2011, Boston Children's implemented the use of radiofrequency (RF) surgical technology. They use sponges that have radiofrequency and can be detected with the use of a wand at the end of the procedure. Also, sponges are stored individually in a digital pocketed holder system from Xodus Medical. "The whole team can see all 10 sponges, for example, because they are visible in the pocketed holder," Norton says. *(For more information on radiofrequency and other tips for avoiding retained items, see package of stories in the September 2009 issue of* Same-Day Surgery, *beginning on p. 91.)*

**• Add a wound closure timeout.**

The wound closure timeout means that as the

## EXECUTIVE SUMMARY

Boston Children's Hospital reduced the number of incorrect counts and count discrepancies by 50% between 2009 and 2010 and reported no incorrect sponge counts for 2011.

- Staff standardized how they counted and where they documented the counts.
- To reduce distractions, no one answers pages during the counting process, and music is turned down.
- During the wound closure timeout, the team stops while the surgeon explores the wound. The nurses make the count and announce that it is correct.
- Films with labeled and radiographed commonly counted items are available in the radiology computer system for the surgeons and radiologists.

surgeon is preparing to close, the team stops while the surgeon explores the wound to ensure nothing is left behind. The nurses make the count and announce that it is correct. "That was a big push and a big change in practice," Norton says.

This process is embedded into the institution's pediatric surgical safety checklist in the "sign out" segment. *(The Pediatric Surgical Safety Checklist is enclosed with the online issue.)*

**• Use a team approach.**

The surgeon OR leaders bought in to the team approach to counts, Martin says. Additionally, "there were combined ground rounds: anesthesia, nurses, surgeons, and the chief of surgery re-introduced the concept of a team approach to the count process," she says.

**• Reduce staff turnover in cases.**

Staff realized that they had a large number of discrepancies in long procedures lasting eight hours or more. "We tried to reduce amount of staff turnover in those cases," Norton says.

When any staff members change, they ensure the count is correct at that time.

**• Enhance accuracy of your radiograph interpretation.**

The OR risk manager and the lead OR radiology technologist labeled and radiographed commonly counted items to show how they appear on film. These films are available in the radiology computer system, and the surgeon or radiologist can access them as needed. *(A copy of those images is available with the online issue.)*

This system addressed one of Martin's worries. "It's always been a concern of mine that if we called radiology and said we're missing a 'peanut' — even that is noted to be a radiopaque item — but how does it show up?"

Some radiopaque items barely show up on X-ray, she points out.

**• Audit.**

"We did audits in the room to measure compliance with policy and expectations and continue our education to find out where weak links are," Norton says.

If compliance is found in an area for several months, that area is dropped from the audit. *(For more information, see legal case below involving a retained item. For additional information, see "Unintended retentions of foreign bodies increase in 2010, even higher in 2011 — What strategies will stop this sentinel event?" SDS Accreditation Update supplement, December 2011, p. 1, and "Procedures, technology can prevent retained items,"* Same-Day Surgery, *September 2010, p. 106.)* ■

# Hospital, surgeon liable for sponge left in patient

*Verdict: $25,000 against each defendant*

By **Jonathan D. Rubin**, Esq.
Partner
Kaufman Borgeest & Ryan
New York, NY

**Sandra L. Brown**, Esq.
Associate
Kaufman Borgeest & Ryan
New York, NY

**Alvin Safran**
Director of Risk and Claims Management
The New York Hospital Medical Center of Queens
Flushing, NY

In 2008, a 27-year-old patient weighed more than 200 pounds when she decided to have a lap band procedure performed.

On June 2, 2008, the surgeon laparoscopically performed the lap band surgery. The surgical procedure was minimally invasive. Two hospital employees assisted the surgeon.

It was undisputed that a three-part procedure exists at the hospital to keep an accurate count of sponges used during surgery. The first count occurs at the beginning of an operation before the patient enters the operating room. In the first count, the surgical technician and the circulating nurse count all the sponges. The surgical technician counts out loud while touching each of the individual sponges as the nurse looks over his or her shoulder. When the surgical technician completes the oral count, the circulating nurse enters

## EXECUTIVE SUMMARY

A gastric banding patient sued her surgeon and hospital for leaving a sponge inside her after surgery.
• The surgeon argued he was less culpable than the hospital, because it was the hospital staff's duty to count the sponges.
• A state court following prior case law assigned equal blame to the hospital and surgeon.
• The patient settled with the surgeon for an undisclosed amount, but the trial court determined that both defendants were equally liable for the error and ordered them to pay $25,000 each in damages.

the specific number of sponges on a white board so that the surgeon is able to see that a count has been performed.

The second count occurs after the laparoscopic instruments are removed from the patient and before the incisions are closed. The final count occurs after the incisions are closed but before the surgeon leaves the operating room.

After the surgery, the patient experienced an unexpected discharge. A CT scan revealed the outlines of a sponge, and the surgeon removed it in a laparoscopic exploratory procedure. The patient filed suit against the surgeon and hospital, and she stipulated that her claim did not equal or exceed $50,000.[1] The chief claim of the plaintiff's suit was that her surgical scar from the gastric banding procedure was now a bit longer.

The surgeon who testified in the case maintained it is the job of the hospital staff to keep track of sponges while the surgeon peers through a laparoscope. In this particular surgery, the surgical technician and the circulating nurse counted the number of sponges three times during the procedure, court records say. The surgical technician counted out loud, while the nurse looked over his shoulder and wrote the number on a white board.

The hospital argued that surgeons should never completely rely on hospital staff to make sure all sponges are out. The hospital further argued that a surgeon is obligated to make his or her own independent check after surgery, which complements the staff's sponge count. The hospital also argued that with laparoscopic surgery, it is impossible for the surgeon to be absolutely sure that all sponges have been removed. The hospital argued that in gastric banding surgery, the incision is just 2 fingertips wide. Any sponge left behind is the size of an egg yolk, and an obese patient has extra layers of fat, which requires a deep incision that is hard to explore thoroughly, the hospital maintained.

The patient settled with the surgeon for an undisclosed amount. At trial, the plaintiff argued that the hospital should be held 100% liable for the damages caused. However, the trial court determined that both defendants were equally liable for the error and ordered them to pay $25,000 each in damages. In doing so, the court ruled that the hospital was not 100% liable and should pay only 50% of the damages, or $25,000.

The judge explained that in such cases, it is rare for one party to shoulder a larger amount, plus the surgeon had a duty to check for sponges himself. The decision is silent on whether the surgeon's original settlement was disrupted by the verdict.

The patient appealed the decision and argued that the hospital should pay a higher proportion of the damages because it was primarily the job of the hospital staff to check for sponges. The appeals court upheld the trial court's decision in an Oct. 5, 2011, decision. The plaintiff's attorney has asked the Louisiana Supreme Court to hear the case. However, in this jurisdiction, few cases are granted appellate review. *(For explanation of what this case means for outpatient surgery programs, see story, below.)*

REFERENCE

1. Louisiana Court of Appeal, Third Circuit. No. 11-0318. ■

# Best practices avoid retained sponges

By **Jonathan D. Rubin**, Esq.
Partner
Kaufman Borgeest & Ryan
New York, NY

**Sandra L. Brown**, Esq.
Associate
Kaufman Borgeest & Ryan
New York, NY

**Alvin Safran**
Director of Risk and Claims Management
The New York Hospital Medical Center of Queens
Flushing, NY

A foreign object retained after surgery always has been a liability difficult to defend. It has been classified as a healthcare-acquired condition.

In a recent case involving a sponge retained after a lap band surgery, it was the court's opinion that the surgeon shared culpability with the hospital.[1] This type of event not only is potentially compensable, but it also has financial implications for reimbursement by Medicare and Medicaid.

Much has been written about what should be done when there is a discrepancy between the initial and subsequent counts. One study conducted in 2003 indicated that 88% of retained foreign objects occurred in counts that were believed to have been correct.[2]

Consider the following sequence of events and how difficult it would be to detect the retained sponge: Five sponges are used, but they initially are counted

incorrectly as four sponges. One of the five sponges is inadvertently is left in the patient. The final count shows four sponges and agrees with the incorrect initial count.

Some gold standard practices for the initial count include:

- The count should be conducted before the case begins and, if possible, before the patient enters the operating room.
- Packaging of devices should be carefully observed and examined.
- Two people should observe the initial count together.
- The items must be carefully separated by one of the two people performing the count.
- The policy and procedure for surgical count should clearly list the emergency conditions under which an initial count will not be undertaken. In that instance, an X-ray must be taken after the procedure.

Historically, the "captain-of-the-ship" approach to a surgical count held the surgeon completely or largely responsible for the accuracy of the count. The rationale was a commonsense approach that the person who inserted the object should be responsible for removing it. Recently that philosophy has shifted. It now is often the perception that the surgical count is the OR staff's responsibility. Again, this is a commonsense thought process that the people who are actually counting the objects that are inserted should be responsible for the accuracy of the count.

In the above cited case, and most established precedent, the surgical count is a shared responsibility between the surgeon and OR staff.[3-5] Surgeons should make sure they follow their hospital's policy with respect to a post-procedural X-ray. Some of the surgeon's responsibilities during the surgical count include: the surgeon determines that an emergency exists requiring a curtailment of the counting process, and the surgeon must conduct a thorough exploration of the surgical wound prior to closure regardless of whether or not the count appears to be correct. To the extent possible, such exploration should be visual and manual.

In a scenario in which the initial count is short by one and an item is left in the patient, thus making the count appear correct, the thorough exploration of the surgical wound would provide the best opportunity for discovering the retained object. In the above-cited case, the court ruled that the physician had the duty to examine for the sponge even though the surgery was laparoscopic.

There are technological advances designed to reduce the possibility of an incorrect count. Bar coding allows individual sponges to be scanned to eliminate the possibility of counting a sponge twice. A master tag containing all of the codes for each sponge in a package also can be used. This system, we hope, would reduce the likelihood of missing one sponge because two are stuck together. Another new technology involves sponges with radiofrequency tags that can be detected by wands.

The prevention of retained foreign objects remains a responsibility for OR staff and surgeons.

## REFERENCE


1. Louisiana Court of Appeal, Third Circuit. No. 11-0318.
2. Gawande AA, Studdert DM, Orav EJ, et al. Risk factors for retained foreign bodies after surgery. *NEJM* 2003; 348(3):229-235.
3. Grant v. Touro Infirmary, 223 So.2d 148 (La.1969), overruled on other grounds by Garlington v. Kingsley, 289 So.2d 88 (La.1974).
4. Guilbeau v. St. Paul Fire and Marine Ins. Co., 325 So.2d 395 (La. App. 3 Cir. 1975).
5. Chappetta v. Ciaravella, 311 So.2d 563 (La.App. 4 Cir 1975)]. ■


# Background checks useful, but limited

About 73% of employers conduct criminal background checks on all job candidates, according to a 2010 survey by the Society for Human Resource Management, and another 19% of employers do so only for selected job candidates. They can be particularly important in healthcare when a job applicant must be trusted with vulnerable patients and data, but experts caution that background checks have limitations.

Background checks are allowed in almost all states, and some states require checks for some healthcare positions, says **Edward F. Harold**, JD, a partner with the law firm of Fisher & Phillips in New Orleans. The Equal Employment Opportunity Commission (EEOC) doesn't prohibit their use, but it recently issued new guidance that discourages using background checks too broadly. *(See the story on p. 77 for more on the EEOC guidance.)*

To best use background checks, first make sure to use a reputable company that can access far more information than you would be able to find on your own, Harold says. Remember that some criminal convictions might not show up in the search because there is no single repository of the data.

Civil offenses also might not show up because some, such as a domestic disturbance resulting in a restraining order, might not be recorded in the crimi-

EXECUTIVE SUMMARY

Criminal background checks can be a useful management tool, but their effectiveness is limited. Do not depend on them to detect all criminal history.
- The Equal Employment Opportunity Commission (EEOC) recently issued new guidelines on using background checks.
- Use a reputable company to conduct the checks.
- Have a policy that dictates exactly how the information will and will not be used.

nal record, explains **Sandy Glover**, CEO of Gold Shield Legal Investigations in Ormond Beach, FL, which performs background checks. "I also recommend checking their professional licensure," Glover says. "Are they really a nurse? Is their license in good standing? Credit reports also can be useful if this person is going to be a position in which they could take advantage of vulnerable people, such as an Alzheimer's patients."

Most employers restrict their searches to convictions, not arrests, because the EEOC has made clear that it sees the use of arrests as highly discriminatory against minorities, Harold explains. *(Some employers are beginning to ask applicants for access to their social media accounts to check for negative information. See the story on right for more on accessing social media.)*

Even restricting the search to convictions can have an adverse impact on minorities and men, because they often have more convictions, notes **David Christlieb**, JD, an attorney with the law firm Littler in Chicago. But conversely, a healthcare employer takes a risk by not conducting background checks.

"The checks are so common now that it would be simple for a plaintiff's attorney to ask why you didn't know that the person you hired had a shady background and then he harmed a patient," Christlieb says. "If you are not required by your state legislature to do background checks, it is still almost expected in the sense that it has become the standard in healthcare to do this. The real question is exactly how you conduct them and what you do with the information."

No matter how you use background checks, have a policy in place before you start checking.

"You must know what you're checking for, how you're checking, and what you will do with what you find. You have to know beforehand how you will respond to certain findings in a background check," Harold says. "Deciding the first time that information appears will only get you in trouble. Consistency is key to avoid charges of discrimination." ■

# No need to check applicants' social media

Some employers are taking advantage of people's tendency to post explicit and sometimes disparaging information about themselves on Facebook and other media by demanding access to those sites before hiring. After incidents in which patient information was posted on Facebook, some healthcare providers might consider monitoring employee sites on an ongoing basis.

Not really a good idea, advises **Edward F. Harold**, JD, a partner with the law firm of Fisher & Phillips in New Orleans.

"The law allows you to ask if you want, but we advise clients not to. You may be taking on more responsibility than you realize," Harold says. "If you have access to his Facebook, but you don't bother to check it for 18 months, and then the employee does something criminal, you could be asked why you didn't see his posts about how he was going to shoot up the place. You had his password, and you could have seen the warning signs."

Demanding access also could drive away otherwise good employees who think it's just too intrusive, Harold says. "Generally, if someone is posting something on social media that has any real bearing on their work performance or trustworthiness, you'll hear about it from coworkers," he says. "It's better to hear about that way than to take on the responsibility of monitoring everyone's social media." ■

# Enforcement guidance targets background checks

Healthcare providers using criminal background checks should take notice of enforcement guidance on employer use of arrest and conviction records in employment decisions. Previous arrests and convictions might not be relevant to the current job application, the Equal Employment Opportunity Commission (EEOC) says in Title VII of the Civil Rights Act of 1964, issued in April 2012 by the EEOC.

The new guidance clarifies and updates the EEOC's longstanding policy concerning the use of arrest and conviction records in employment, EEOC Chair **Jacqueline A. Berrien** said in announcing the update. While Title VII does not prohibit an employer from requiring applicants or employees to provide information about arrests, convictions, or incarceration, it

is unlawful to discriminate in employment based on race, color, national origin, religion, or sex. The guidance builds on guidance documents that the EEOC issued more than 20 years ago that explained when the use of arrest and conviction records in employment decisions might violate Title VII.

Unlike previous enforcement guidelines, the new guidance urges employers not to automatically disqualify applicants when criminal records are found, even if the charges or convictions were of a serious nature. Employers should give applicants a chance to explain a report of past criminal misconduct before they are rejected outright, the EEOC says. An applicant might say the report is inaccurate or point out that the conviction was expunged, it might be completely unrelated to the job, or the applicant might show he or she has been fully rehabilitated, the EEOC explains.

The EEOC also recommends that employers stop asking about past convictions on job applications. Additionally, it says an arrest without a conviction is generally not an acceptable reason to deny employment.

The materials for the public meetings held on the use of arrest and conviction records, including testimony and transcripts, are available at http://eeoc.gov/eeoc/meetings/index.cfm. ■

**Same-Day Surgery Manager**

# Use these reports to monitor surgery stats

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

If your facility is open as you read this, congratulations! There are a number of freestanding facilities that didn't make it through the past "dark years." Not quite sure what else to the call the past three years, but not a lot of points of light came through. Many hospitals had cutbacks and staffing "brown outs" (the staffing equivalent of electrical rolling brown out.) So if you are reading this column, that is great news. Good to see you are still here.

I am a huge advocate of management "report cards" for hospital and freestanding units. They are very simple to establish, they allow for most staff members to participate, and they offer a reliable and accurate portrayal of how your department or facility is doing from several different angles.

This report, again, is simple to use and is really a great way to get unmotivated staff members involved in the operational side of the business. You have to be willing to share some information, but there is nothing wrong with your staff understanding the viability and health of your operations. Look at the millions of employees in publicly traded businesses in the United States. Those individuals merely need to go online to see all kinds of information about how those companies are doing in the stock reports. So, secrecy isn't what it used to be. Business transparency is good.

Start with your revenue. Everyone has a budget. How much money are you supposed to bring in each year, month, and week? Set it up in an Excel or Numbers spreadsheet for each month. Now put in how much you actually collected. Rarely do they jive. Why didn't they? Unplanned surgeon vacation? Falling out with a payer? Jot down the explanation. Many times there may be a difference or "variance" between the two that can be explained. While you are doing this, what is the percentage of the change? Often there can be a lot of money difference, but when you look at the actual percentage difference, it is not all that dramatic. Add that figure to your equation.

You will create something like this:

REVENUE:

| MONTH: | Actual | Budget | Variance | %Variance |
|---|---|---|---|---|
| | $ | $ | $ | |
| YTD: | Actual | Budget | Variance | %Variance |
| | $ | $ | $ | |

Variance Explanation: _____

_____

_____

Keep your explanations short and to the point. This is not a novel.

Since you are looking at the revenue, you need to look at your cases that were budgeted. Use the same format as revenue:

NUMBER OF CASES:

| MONTH: | Actual | Budget | Variance | %Variance |
|---|---|---|---|---|
| | $ | $ | $ | |
| YTD: | Actual | Budget | Variance | %Variance |
| | $ | $ | $ | |

Variance Explanation: _____

_____

_____

It actually starts to become fun. Now, dig deeper! What specialty are you doing more of? Track it like this:

| | Specialty | # of Cases | | % Month Total |
|---|---|---|---|---|
| 1 | | | | % |
| 2 | | | | % |
| 3 | | | | % |
| 4 | | | | % |
| 5 | | | | % |
| 6 | | | | % |
| 7 | | | | % |
| 8 | | | | % |
| 9 | | | | % |
| 10 | | | | % |
| | | | *(total)* | *(total)* |

Now, where is the money being spent from your revenue? Find out by going through the major expenditures. There are many things you spend money on each month. There are often too many to track here, so pick the items on your budget by line on the budget. Your major "line items" are often supplies and personnel. Add them just like you did the above.

Finish it off with something like this:

| Dollars/Dollars Ratio: | Percentage |
|---|---|
| Personnel Cost/Net Revenue | % |
| Drugs & Medical Supplies/Net Revenue | % |
| Other Operatin Expenses/Net Revenue | % |
| Total Operating Expenses/Net Revenue | % |

In other words, what percent of your income or collections is spent on personnel cost? Supplies? What you want to measure is at your fingertips.

Add another line here that measures how much of your income is spent on staff education, conferences, and publications. Take this information to whomever you report to and use it as justification to allocate more funds to staff education.

If your administrator or dreaded VP doesn't share this information with you, then ask to be involved next month. I have never turned down a staff member who wanted to be part of running a facility. Everyone wins! *[Earnhart & Associates is a consulting firm specializing in outpatient surgery development and management. Contact Earnhart at Earnhart & Associates, League City, TX. Phone: (512) 297.7575. E-mail: searnhart@earnhart.com. Web: www.earnhart.com.]* ■

# Did you receive ebulletin from us?

On May 10, we sent out email about final Medicare regulations that will result in changes for ambulatory surgery centers and hospitals. If you didn't receive it, we don't have your email address. Contact out customer service department at (800) 688-2421 or customerservice@ahcmedia.com. ■

## CNE/CME INSTRUCTIONS

Physicians and nurses participate in this CNE/ CME program and earn credit for this activity by following these instructions.

1. Read and study the activity, using the provided references for further research.
2. Log on to **www.cmecity.com** to take a post-test; tests can be taken after each issue or collectively at the end of the semester. *First-time users will have to register on the site using the 8-digit subscriber number printed 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 last test of the semester, your browser will be automatically directed to the activity evaluation form, which you will submit online.
5. Once the completed evaluation is received, a credit letter will be e-mailed to you instantly. ■

## COMING IN FUTURE MONTHS

- How to avoid financial pressures to release patients too early
- What to expect with upcoming infection control survey
- Tips on preventing venous thromboembolism
- New resource targets OR medication safety

# CNE/CME OBJECTIVES

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

# CNE/CME QUESTIONS

1. Which of the following statements is true concerning the disks involved in the data breach at Emory Healthcare, which cost the facility between $1.5 and $2 million?
   A. The discs were in an office cabinet that was not locked at night, but they were encrypted.
   B. The discs were in an office cabinet that was not locked at night, although it was on a restricted hallway
   C. The discs were in an office cabinet that was locked at night, but it was on an unrestricted hallway.
   D. None of the above.

2. Which of the following is true of the process that resulted in reducing incorrect counts and count discrepancies by 50% between 2009 to 2010 at Boston Children's Hospital?
   A. Staff determined they needed standardization in how they counted.
   B. B. Staff determined they needed standardization in where they documented the counts.
   C. A and B
   D. Neither A nor B.

3. A gastric banding patient sued her surgeon and hospital for leaving a sponge inside her after surgery. What was the outcome?
   A. The surgeon was found responsible.
   B. The hospital was found responsible.
   C. The patient settled with the surgeon for an undisclosed amount, but the trial court determined that both defendants were equally liable for the error and ordered them to pay $25,000 each in damages.

4. Which of the following is true regarding the recent guidance from the Equal Employment Opportunity Commission regarding criminal background checks of job applicants?
   A. The new guidance urges employers not to automatically disqualify applicants when criminal records are found, even if the charges or convictions were of a serious nature.
   B. The new guidance clarifies that there is not risk in automatically disqualifying applicants when criminal records are found, particularly if the charges or convictions were of a serious nature.
   C. The new guidance encourages employers to consider previous arrests, not just convictions, when considering applicants.
   D. The new guidance discourages employers from using criminal background checks in any way because they can be disproportionately harmful to minorities.