SAME-DAY SURGERY

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

OCTOBER 2016 Vol. 40, No. 10; p. 109-120

INSIDE

AHC Media

Ransomware at Surgery Center Raises Question of Vulnerability

Two recent ransomware attacks at ambulatory surgery centers have managers wondering how to prevent or, if necessary, respond to such attacks.

In a ransomware attack, hackers seize control of a facility's computer system and records, then demand payment for the installed encryption key so the facility can regain control of its own computer system.

Facilities pay the ransom through a pre-paid cash voucher or bitcoin, which is a decentralized network that has its own currency. Some ransomware works via email attachments, according to The Doctors Company, the nation's largest physician-owned medical malpractice insurer. The insurer, based in Napa, CA, recently released a cybersecurity guide.[1] *(See information about the guide in the resources listed at the end of this article.)*

"ALMOST ALL HEALTHCARE PROVIDER ORGANIZATIONS HAVE BEEN BREACHED OR SUFFERED AN ATTACK IN THE LAST TWO YEARS."
— ELLEN M. DERRICO

"If the organization has performed frequent system backups, it can typically restore its data with limited loss," according to The Doctors Company. "However, if backups are not performed, the ransom must be paid or the organization must reset its system back to its default setting — and lose everything."

Consider these recent examples of ransomware:

- Staff members at The Ambulatory Surgery Center at St. Mary in Langhorne, PA, discovered a malware breach June 1 when they noticed encrypted files on an internal network, according to a newspaper report.[2] The center is owned by a hospital and local physicians. The center had backed up all of its files,

NOW AVAILABLE ONLINE! **VISIT** AHCMedia.com or **CALL** (800) 688-2421

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

SAME-DAY SURGERY

Same-Day Surgery®,
ISSN 0190-5066, is published monthly by AHC Media, LLC, One Atlanta Plaza, 950 East Paces Ferry Road NE, Suite 2850, Atlanta, GA 30326

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

POSTMASTER: Send address changes to:
SAME-DAY SURGERY
P.O. Box 550669
Atlanta, GA 30355

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

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

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

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

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

Provider approved by the California Board of Registered Nursing, Provider #CEP14749, for 1.75 Contact Hours.

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

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

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

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

EXECUTIVE EDITOR: Joy Daughtery Dickinson
Joy.Dickinson@AHCMedia.com
DIRECTOR OF CONTINUING EDUCATION AND EDITORIAL: Lee Landenberger.

PHOTOCOPYING: No part of this newsletter may be reproduced in any form or incorporated into any information retrieval system without the written permission of the copyright owner. For reprint permission, please contact AHC Media, LLC. Address: P.O. Box 550669, Atlanta, GA 30355. Call: (800) 688-2421. Web: AHCMedia.com.

Copyright © 2016 by AHC Media, LLC. *Healthcare Risk Management*™ and *HRM Legal Review & Commentary*™ are trademarks of AHC Media, LLC.
Same-Day Surgery® is a registered trademark of AHC Media, LLC. The trademark *Same-Day Surgery®* is used herein under license. All rights reserved.

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

so it restored them the same day and didn't pay the cybercriminals, according to the news report.

The surgery center leaders are certain that medical records and patient charts weren't accessed because they keep them on a separate network. However, the leaders weren't certain whether the cyberattackers had accessed data such as patient names and dates of birth, so they offered 13,000 patients who were affected a year of free identity theft protection, credit monitoring, and identity restoration, the newspaper reported. Although the surgery center didn't release the cost of these services, they generally run $10-$20 per patient, according to sources.

Patients also were given access to a toll-free number to call.

• Athens (GA) Orthopedic Clinic, which includes an outpatient surgery center, experienced a ransomware attack of about 397,000 current and former patients that was discovered June 28. "The breach occurred when a hacker used the credentials of an outside contractor who performed certain services for the Clinic," the center said in a prepared statement.

The clinic "immediately hired cyber-security experts and notified the FBI," it said. At that time, the center didn't disclose the breach publicly because, it says, it didn't want to interfere with its investigation "or push the hacker into a mass public release of data."

Several days later, the center confirmed the EMRs had been hacked. It took several weeks to determine what patients and data were affected, it says. While it was compiling lists of the affected patients to mail notices to them, it learned the hackers, who call themselves the "Dark Lords," were attempting to sell the data on the black market. "[W]e immediately issued a press release, put statements on our website and Facebook page, and continued trying to get letters mailed," the center said. The center offered information about how patients could protect themselves.

Both centers have taken steps to address security vulnerabilities, they report.

Fastest Growing Threat

Ransomware is the fastest growing malware threat, according to a recent technical guide developed the departments of homeland security, justice, and health and human services. *(For information about the guide, see the resource list at the end of this article.)*

"Almost all healthcare provider organizations have been breached or suffered an attack in the last two years," says **Ellen M. Derrico**, MBA, a marketing/market development

EXECUTIVE SUMMARY

Two recent ransomware attacks at surgery centers have managers wondering how to prevent or, if necessary, respond to such attacks.

- Identify your highest risks: medical devices, the network, mobile devices, your staff, outside contractor, or vendors.
- Use intelligent firewalls. Install updates and patches to software on a regular basis. Use backup software.
- Consider using Mac devices. If you use Microsoft, disable your macros.

executive in healthcare and life science technologies and an independent consultant in West Chester, PA. "Many have had multiple attacks per year, month, week, and even per day."

More than half of all healthcare provider organizations have reported finding traces of malware and viruses on devices on their networks, Derrico says. "Some of this malware and viruses are just waiting to execute," she says.

And it's not just patient's identities that are at risk. Ransomware attacks directly threaten patient safety, Derrico says.

One hospital that experienced a ransomware attack was without access to email and electronic health records for 11 days, with clinicians left to rely on faxes and verbal communication. New records and patient registration information were recorded on paper, and some patients were transferred to other hospitals. It is only a matter of time before a ransomware attack causes serious harm or death because clinicians were unable to access records about a patient's history, status, or medication administration, Derrico says.

Another concern is the expense. "On average, a basic breach costs $3.7 million to clean up, and then when records are stolen, you end up with lawsuits," Derrico says. "When you add up all the costs and liability from a ransomware attack, it's even worse. It can be catastrophic to a healthcare organization."

Outpatient Is Vulnerable

As if the news couldn't get any worse, outpatient surgery settings might be particularly vulnerable to a ransomware attack, say sources interviewed by *Same-Day Surgery.*

"Same-day surgery facilities may have an increase in vulnerability, due to the volume of patients, the increased mobility of the clinicians, and the level of security in place," Derrico says.

Another area of vulnerability is the type of critical medical equipment found in surgery centers, says **Erik Rasmussen**, JD, cyber practice leader with Kroll's Cyber Security and Investigations practice, based in the Los Angeles office. Rasmussen is a former deputy prosecuting attorney and special agent with the U.S. Secret Service, where he focused primarily on domestic and international computer crime investigations. Earlier in his career, Rasmussen served on the Los Angeles FBI Joint Terrorism Task Force, where he investigated activities of domestic and international terrorist organizations.

"ON AVERAGE, A BASIC BREACH COSTS $3.7 MILLION TO CLEAN UP, AND THEN WHEN RECORDS ARE STOLEN, YOU END UP WITH LAWSUITS."

"Critical medical equipment, such as what you would find at an ambulatory surgery center, is generally at risk due to the sensitive nature of the applications on that equipment," Rasmussen says. "The applications often preclude traditional antivirus, anti-malware software, or normal patching timetables." Examples include drug infusion pumps and any other network-enabled equipment.

A surgery center co-owned by a hospital or part of an integrated delivery system, where patient records are shared across entities and where networks and IT systems are shared, might be particularly vulnerable, Derrico says. Such a setting offers "the highest potential for a bountiful attack, yielding the most records in a theft scenario and the most opportunity for extortion in the ransom scenario," she says.

The bottom line? "All healthcare providers are targets on one level or another," Derrico says. *(See stories about preventing attacks, responding to attacks, training, and security breaches in this issue.)* ■

REFERENCES

1. The Doctors Company. Cybersecurity and data breaches. Strategies to mitigate risk, monitor security, and respond in the event of a cyberattack. August 2016. Accessed at http://bit.ly/2bSCiCk.
2. Wagner J. Ransomware attacks info of 13K patients at Ambulatory Surgery Center at St. Mary. *Bucks County Courier Times*: July 11, 2016. Accessed at http://bit.ly/2bQcrtK.

RESOURCES

- The cybersecurity guide from The Doctors Company is available online at http://bit.ly/29zm57B.
- The federal guidance can be accessed at http://bit.ly/2966w4T.
- For cybersecurity resources from the American Hospital Association, visit www.aha.org/cybersecurity.

SOURCE

- **Ellen M. Derrico**, MBA, Marketing/Market Development Executive, Healthcare and Life Science Technologies, West Chester, PA. Email: ellenmd1@gmail.com.

How Outpatient Surgery Programs Can Prevent Ransomware Attacks on Their Programs

Do you want a 100% effective method for preventing ransomware? It doesn't exist, according to **Ellen M. Derrico**, MBA, a marketing/market development executive in healthcare and life science technologies and an independent consultant in West Chester, PA.

The reason is that "ransomware is a form of malware that can get into an organization a number of ways: insiders innocently clicking on a phishing email or malware advertisement, hackers hacking in, a medical or mobile device connecting to the network, and it goes on and on," Derrico says.

However, there are steps you can take to reduce your risk, she and other sources emphasize. Consider the following tips:

• Evaluate your risk.

The first step is to assess your environment, Derrico advises. "[T]ake stock in what you currently have in place for cybersecurity from a technology, training and education, vulnerability testing, and backup-plan perspective," she says.

Identify your highest risks, Derrico suggests. "Is it the medical devices, the network, the mobile devices, the people, outside contractors, and vendors?" she asks. "Find the intersection of your capabilities for cybersecurity and your risks, so you can see what is not currently being addressed."

• Compare your facility with those of your peers.

Benchmark your program with similar ones, Derrico suggests. "There are companies and vendors who are currently offering free assessments and benchmarking to help you," she says. "Take advantage of this to quickly get an idea of where you are and where you need to be." *(See two options listed as resources at the end of this article.)*

Next, talk to leaders at similar facilities, Derrico says. "Call up other, non-competitive surgery centers in other states and ask them what they are doing," she suggests.

Don't limit yourself to surgery centers, however, Derrico advises. "Consider talking with regional medical centers that are on tight budgets and are smaller than integrated delivery systems," she says. "They can tell you a lot about where they see the biggest bang for the buck, where to spend, and what to do to mitigate your risk from a real-world perspective."

• Network.

Become involved with the regional group for the Healthcare Information and Management Systems Society in Chicago. "Many folks attend these meetings and share best practices, plus they know other folks and can network you in," Derrico says.

Also, attending national and global conferences will allow you to connect with people from other regions who are less competitive and can share their best practices freely. "If you don't have time or budget for travel, attend online seminars and events to connect with folks through these venues and through social [media]," she says.

Use social networks such as LinkedIn to ask questions in group discussion areas, Derrico advises. "You will be surprised how much feedback you will get and how helpful it can be," she says.

• Use the right technology.

Use intelligent firewalls to block malware, The Doctors Company advises in a just-released cybersecurity guide.[1] Also, use intrusion detection software that can monitor illegal activities on networks, the company says. "Stop malware from executing on desktop computers by installing application whitelisting software, anti-virus, or anti-malware," it says.

Install updates and patches to software on a regular basis, The Doctors Company advises. "These include patches that fix vulnerabilities in the software, helping support your antivirus software, your firewall, and all other security measures," it says.[1]

Also, use Mac devices, advises **Tom Kellermann**, CISM, chief executive officer at Strategic Cyber Ventures, a cybersecurity-specific investment fund based in Washington, DC. Mac devices "are 80% less vulnerable to ransomware attacks because they do not automatically run executables," which are computer files that are in a format ready for execution, Kellermann says. There are only two ransomware variants that attack Macs, and end-point security from companies such as Invincea, based in Fairfax, VA (www.invincea.com), and Trend Micro, based in Irving, TX (www.trendmicro.com), can prevent ransomware from spreading and encrypting files, he says.

If you use Microsoft, disable your macros, Kellermann advises. Go to the "Trust Center," "Trust Center Settings," and then "Macro Settings."

Also, use backup software, Kellermann advises. In the event you have been successfully attacked via ransomware, restore the machine's images and data from backup and then run a security scan, he says.

• Migrate your systems, both

software applications and data, to the cloud.

This advice for small practices comes from The Doctors Company, which advises providers to "fully vet your storage cloud vendor.[1] *(The guide offers a section on strategies for vendor selection.)*

If you can't store data in the cloud, then consider working with a computer forensic firm so you'll have strong capabilities for security and investigations, The Doctors Company advises.

Chris Johnson, medical IT consultant and director of strategy and business development of Wheelhouse IT, formerly Untangled Solutions, in Fort Lauderdale, FL, spoke at the Ambulatory Surgery Center Association meeting this year and reported that he is working with a security firm that is taking the elements that protect an outpatient surgery program and giving them a perimeter that sits on the cloud. "What it does is, instead of having all of those bad things hit your physical perimeter, it hits out there first and gives you that added security buffer before it ever gets through that front door," Johnson said. The technology that is coming is getting less expensive, he said. "The technologies are getting more robust, and we can actually fight the bad guys," he said. "We don't have to be the victims of ransomware." ■

REFERENCE

1. The Doctors Company. Cybersecurity and data breaches. Strategies to mitigate risk, monitor security, and respond in the event of a cyberattack. August 2016. Accessed at http://bit.ly/2bSCiCk.

RESOURCES

- Intel Health and Life Sciences in Santa Clara, CA, is offering healthcare providers a free one-hour cybersecurity assessment with partner technology companies in an open industry collaboration. Web: www.Intel.com/BreachSecurity.
- RSA in Bedford, MA, has an online cybersecurity maturity assessment survey. Web: http://bit.ly/1rz32hh.

Prevent Ransomware With Policies, Plus Fun Training

To avoid a ransomware attack, put together a holistic cybersecurity program that fits your budget and addresses your highest areas of risk, suggests **Ellen M. Derrico**, MBA, a marketing/market development executive in healthcare and life science technologies and an independent consultant in West Chester, PA.

"If it is your people, focus on education and training," she says. "Keep it simple, fun, and low cost, but make it effective."

Phil Alexander, information security officer and director of information security at UMC Health System in Lubbock, TX, runs a competition on phishing and publishes the results in a *Phish Market* newsletter. IT security staff create phishing emails and send them to staff from what appears to be outside email addresses. They are "trying to look as legitimate as possible to see who they catch," Derrico says.

The staff monitor who clicks on the links. Those who do not click end up in the *Phish Market*, and they also receive a T-shirt, Derrico says. "The competition has raised the visibility of phishing, the most popular way of infecting devices and getting ransomware into a network," Derrico says. "It has also reduced phishing success by over 70% and increased the clinician satisfaction with IT by 88%."

Alexander also runs a competition mimicking the characters in the "Men in Black" movie who are in search of "aliens," which are suspicious downloads and USBs, infected devices, and other items. "When someone calls his department or emails to report something suspicious — an alien — he and his team show up dressed like the 'Men in Black' and give out a toy alien to put next to the computer or other infected device," Derrico says. "The clinicians really seem to love it, and his department has earned their support and trust."

More than 80% of cyberattacks can be attributed to human error or human involvement, according to The Doctors Company, in a just-released cybersecurity guide.[1] "Provide ongoing security awareness for all employees," the guide says. "Train staff members to avoid downloading, clicking on links, or running unknown USBs on computer systems."

Make sure your policies and procedures for mobile and medical devices are robust, Derrico says. For example, perform an audit of your devices, including mobile and medical devices, she says. "Make sure all devices have the most current version of software, operating systems, and apps installed to prevent attacks/be most current," Derrico says. "Talk with your vendors of mobile and medical devices to identify vulnerabilities … and work toward fixing these vulnerabilities or replacing your devices with newer, more robust devices."

Your firmware should be up to date, Derrico says. Firmware is a

software program or instructions that explain how the device communicates with other computer hardware. Also, ensure you can quickly quarantine an infected device, Derrico says.

"Make sure sensitive data are encrypted and access is well-managed, restricted, where need be, and governed," she says. "The bottom line: Know where you stand, and be ready to make the right investments in security."

If you don't have your own IT staff, consider engaging an outside technology/IT expert who performs upgrades, tests the system for vulnerability, and is available to rapidly respond should a problem occur, suggests **Mark Mayo**, CASC, the ASC administrator at Chicago Surgical Clinic in Arlington Heights, IL. "This way, your expert is already familiar with your system, its architecture, and the programs you routinely run," Mayo says.

Draft a written incident response plan for cyberthreats, and update these plans regularly, says **Erik Rasmussen**, JD, cyber practice leader with Kroll's Cyber Security and Investigations practice, based in the company's Los Angeles office. "Facilities should conduct simulated attacks, and we suggest using the tabletop exercise model to learn from these scenarios," Rasmussen says.

If the highest area of risk is technology, use penetration testing, also called pen testing, to identify the weakest links that need to be fixed, Derrico suggests. These pen tests can be automated with software applications, or they can be performed manually. "In addition to being ready for it, surgery centers need to lobby hard for resources — money and people — to provide technology, training, and expertise on vulnerability testing and on security," Derrico says, "So get your C-suite involved, help educate them on the cost, the need, and the benefits, including mitigating risk of an attack and preventing the cost of the attack and compliance violations." ■

REFERENCE

1. The Doctors Company. Cybersecurity and data breaches. Strategies to mitigate risk, monitor security, and respond in the event of a cyberattack. August 2016. Accessed at http://bit.ly/2bSCiCk.

When a Ransomware Attack Occurs, What Steps Does Your Facility Need to Take?

If your facility's computers are infected with ransomware, you should report the incident immediately to your FBI Field Office Cyber Task Force or Secret Service field office, according to technical guidance developed by the departments of Homeland Security, Justice, and Health and Human Services summarizing best practices to prevent and respond to ransomware. *(The guidance is available online at http://bit.ly/2966w4T.)*

For information on contacting the FBI office, go online to the website http://bit.ly/2blgpxu. For information on contacting the Secret Service, go to http://bit.ly/2cb5OGT. Also, go to the FBI Internet Crime Complaint Center at http://bit.ly/1eTje5I, the agencies advise.

Should you pay the ransom? No, according to a joint alert from the U.S. Department of Homeland Security and the Canadian Cyber Incident Response Centre. "Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information," the alert says. "In addition, decrypting files does not mean the malware infection itself has been removed." *(The alert is available at http://1.usa.gov/1RBQRWD.)*

Ellen M. Derrico, MBA, a marketing/market development executive in healthcare and life science technologies and an independent consultant in West Chester, PA, says "Many experts are writing, blogging, and speaking on why it is better to not pay the ransom — 'don't negotiate with terrorists.' But in healthcare, where innocent lives may be at risk if the system goes down and they are in a critical situation — coding, ICU, ED, or OR — then you need to be able to move fast."

Because every second counts, "it is so critical to know where you stand and know which decision to take, based on your organization's ability to sideline the ransomware attack," Derrico says.

Have your plan ready. "The key is when it does happen, how fast can you detect and shut it down, quarantine the rest of your network and devices?" Derrico says. "If you are ready for it and you have a solid plan B to quarantine affected devices, areas of the network, systems, etc., you have everything backed up and

accessible somewhere else — the cloud for example — and your people can move fast so as to not put any patient at risk, then don't pay the ransom."

If you aren't able to quickly stop the spread of the ransomware and you don't have a plan to be up and running again in seconds, "then you have to consider paying the ransomware quickly, before the criminals move on and are gone, and before patients are adversely affected," she says. "The trick here is, again, to know where you stand." ■

OCR: Ransomware Attack Usually a Data Breach

With ransomware attacks a continuing threat to healthcare providers, the Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) is warning that, in addition to all the other headaches, such incidents could be considered a data breach under HIPAA.

Responding to the threat of ransomware attacks, the OCR has released HIPAA guidance on ransomware. The new guidance points out that a ransomware attack probably means there has been a protected health information (PHI) data breach under HIPAA.

"The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems [sic] is a security incident under the HIPAA Security Rule," the guidance says. "A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

That type of incident would trigger the notification requirements. Organizations experiencing a breach of unsecured PHI must notify individuals whose information is involved in the breach and, in some cases, the media, unless the entity can demonstrate and document that there is a "low probability" that the information was compromised, HHS says.

The guidance suggests conducting a risk analysis to identify threats and vulnerabilities to PHI and establishing a plan to mitigate or remediate those identified risks. In addition, the guidance advises taking these steps:

• Implement procedures to safeguard against malicious software.

• Train authorized users on detecting malicious software, and report such detections.

• Limit access to PHI to only those persons or software programs requiring access.

• Maintain an overall contingency plan that includes disaster recovery, emergency operations, frequent data backups, and test restorations. The guidance is available to readers online at http://bit.ly/29zm57B.

According to just-released guidance from The Doctors Company, the nation's largest physician-owned medical malpractice insurer, "[s]mall practices without sophisticated systems or firewalls may have to hire a forensic computer firm to demonstrate that a breach did not occur."[1]

For a summary of the HIPAA Privacy Rule, readers can go online to http://bit.ly/1ZnuVnN. ■

REFERENCE

1. The Doctors Company. Cybersecurity and data breaches. Strategies to mitigate risk, monitor security, and respond in the event of a cyberattack. August 2016. Accessed at http://bit.ly/2bSCiCk.

ACS Statement on Appropriate Professional Attire For Surgeons Raises Concerns From AORN

The American College of Surgeons (ACS) has released a statement on professional attire for surgeons in and out of the OR, but the Association of periOperative Registered Nurses (AORN) has raised concerns about some recommendations that the organization says are not supported by evidence.

AORN says that of particular concern is the introductory statement, "The ACS guidelines for appropriate attire are based on professionalism, common sense, decorum, and the available evidence."

In a released statement, AORN said, "Regulatory agencies, accrediting bodies, and patients expect healthcare organizations to follow guidelines that are evidence-based rather than recommendations based on professionalism, common sense, or decorum."

All evidence for safe surgical attire

is presented with recommended evidence-based practices in AORN's *Guideline for Surgical Attire*, the organization said.

The individual elements of the statement from ACS and the review of evidence from AORN are listed as follows:

ACS: Soiled scrubs and/or hats should be changed as soon as feasible and certainly prior to speaking with family members after a surgical procedure.

AORN: The Occupational Safety and Health Administration requires attire that has been penetrated by blood, body fluids, or other infectious materials be removed immediately or as soon as possible and be replaced with clean attire.

ACS: Scrubs and hats worn during dirty or contaminated cases should be changed prior to subsequent cases even if not visibly soiled.

AORN: Evidence shows that perioperative team members who are following standard precautions, using personal protective equipment (PPE), and conducting hand hygiene should not need to change scrubs and hats between cases. Doing so could give a false sense of security that PPE and hand hygiene are not needed. This statement may cause confusion by introducing a different standard for surgeons than for other perioperative team members. All should be following the same, evidence-based standards.

ACS: Masks should not be worn dangling at any time.

AORN: Evidence-supported.

ACS: OR scrubs should not be worn in the hospital facility outside the OR area without a clean lab coat or appropriate cover up over them.

AORN: Evidence shows that lab coats can be contaminated with large numbers of pathogenic organisms. Evidence also shows that lab coats are not always discarded daily after use or laundered on a frequent basis and, therefore, should not be recommended wear over scrubs. If one chooses to wear a lab coat, it should be laundered in a healthcare-accredited laundry facility after each daily use and sooner when contaminated, or should be single use.

ACS: OR scrubs should not be worn at any time outside the hospital perimeter.

AORN: Evidence-supported.

ACS: OR scrubs should be changed at least daily.

AORN: Evidence-supported.

ACS: During invasive procedures, the mouth, nose, and hair (skull and face) should be covered to avoid potential wound contamination. Large sideburns and ponytails should be covered or contained. There is no evidence that leaving ears, a limited amount of hair on the nape of the neck, or a modest sideburn uncovered contributes to wound infections.

AORN: As with most other aspects of surgical practice, there are no randomized, controlled trials demonstrating the effect of different types of surgical head covering on surgical site infection rates.

However, there is a body of evidence that supports covering the hair and ears due to the fact that hair and skin can harbor bacteria that can be dispersed into the OR environment. As patient safety is the primary consideration for all perioperative personnel, reducing the risk of patient exposure to microorganisms that are shed from the skin and hair to help reduce the risk of surgical site infection should be a high priority for all perioperative personnel. The ACS statement says "limited amount of hair and modest sideburn can be uncovered." Until an evidence-based definition for "limited" and "modest" can be determined, there is no way for facilities to enforce such a recommendation.

ACS: Earrings and jewelry worn on the head or neck where they might fall into or contaminate the sterile field should all be removed or appropriately covered during procedures.

AORN: Evidence-supported.

ACS: The ACS encourages clean, appropriate professional attire (not scrubs) to be worn during all patient encounters outside the OR.

AORN: No opinion.

ACS: The skullcap is symbolic of the surgical profession. The skullcap can be worn when close to the totality of hair is covered by it and only a limited amount of hair on the nape of the neck or a modest sideburn remains uncovered. Like OR scrubs, cloth skull caps should be cleaned and changed daily. Paper skull caps should be disposed of daily and following every dirty or contaminated case. Religious beliefs regarding headwear should be respected without compromising patient safety.

AORN: See the above statements regarding the enforcement confusion introduced by words such as "limited" and "modest." Wearing a particular head covering based on its symbolism is not evidence-based and should not be a basis for a nationwide practice recommendation. Several types of evidence exist that support recommendations that perioperative personnel cover their head and ears in the OR. This evidence includes the fact that human skin and hair is naturally colonized with many bacteria, and perioperative personnel shed microorganisms into the air around them. We know airborne bacteria in the OR can fall into the operative field, contribute to the overall air contamination of the OR,

and place patients at risk of surgical site infections. Completely covering the hair can reduce the number of bacteria introduced into OR air by perioperative personnel.

The National Guideline Clearinghouse requires guideline developers to examine the risk and benefit of a recommendation to patients and personnel. There is no risk to perioperative personnel to cover their skin and hair, while the benefit of doing so to patients is that it reduces the patient's exposure to potentially pathogenic organisms and helps protect them from harm. Head coverings based on symbolism and a personal attachment to historical norms have no place in the patient benefits analysis expected of guidelines developers by the National Guideline Clearinghouse.

ACS: Many different healthcare providers (surgeons, anesthesiologists, CRNAs, laboratory technicians, aides, etc.) wear scrubs in the OR setting. The ACS strongly suggests that scrubs should not be worn outside the perimeter of the hospital by any healthcare provider. To facilitate enforcement of this guideline for OR personnel, the ACS suggests the adoption of distinctive, colored scrub suits for OR personnel.

AORN: AORN supports this statement; however, nurses and scrub techs should be included in any list of healthcare providers who wear scrubs in the OR.

ACS is working with CMS as well as The Joint Commission so that those groups' policies and regulatory oversight are aligned with the ACS recommendations, the College said in its statement. The ACS statement will be published in the October issue of the *Bulletin of the American College of Surgeons*.

To view the entire statement from ACS, readers can go online to the website http://bit.ly/2aA6ceG. ■

Boost Collections by 634%? Surgery Center At This Hospital Has Done It

Registrars at The Cooper Health System in Camden, NJ, recently began giving patients who are hospital employees a new option: to use one, two, or three payroll deductions to take care of their copays. This seemingly minor change gave revenue a major boost.

Point-of-service collections rose a whopping 634% at the surgical center, reports **Pamela Konowall**, CHAM, assistant director of healthcare access. The following steps also contributed.

The health system attempts to collect copays for same-day surgery patients before the surgery, Konowall says. "A phone call is made the night before the scheduled procedure in an effort to educate the patient and collect," she says.

Patients are encouraged to make payments before they arrive. Staff members explain to patients "that they will not have to worry about bringing valuables such as credit cards when their payment is made before their procedure," Konowall says.

A list of patients who have unpaid copays is distributed to the access department, she says. "The registrar is responsible to request payment upon the patient's arrival the day of surgery," Konowall says.

Top collectors are recognized every week with gift cards or movie tickets. "An email spotlighting the employee is sent to all of their co-workers," Konowall adds.

College Helped Train

A local community college was an unexpected source of help in improving cash collections. Many of the healthcare system's employees attend classes at the school.

"The revenue cycle team was mindful that there have been numerous times the college actually comes on site to conduct classes for hospital staff," Konowall says.

Leaders did some research and discovered that the college had a grant available. Faculty members were willing to provide point-of-service training sessions for registrars. "The college's Office of Customized Training developed the training to meet the needs of collectors per the specifications of the revenue cycle team," says Konowall.

The instructor had a healthcare and sales background. The college didn't charge but required at least 15 people be enrolled. "The idea was to give front-end collectors the *whole* picture," says Konowall. "Topics from the evolution of the payment system to the evolvement of scripting were reviewed."

In February, the college's faculty held eight training sessions for front-end staff at the hospital's Central Business Office. "Immediately following this training, front-end collectors were so excited, they were calling the access management team to report their successes," says Konowall. Registrars learned to build relationships with patients, use

helpful phrases, and address common objections. One registrar excitedly reported making three successful collections. "She stated collecting was much easier than she first thought," says Konowall. ■

SDS Manager

Four Outpatient Surgery Situations You May Encounter and the Best Solutions

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

One of the most popular features in this column is bringing examples of what we are seeing at the 30,000-foot level across 49 states where we have clients. (Come on, Hawaii. Where are you?)

Our approach to issues our clients are facing is sometimes controversial, sometimes right, and sometimes so-so, but it does spawn lots of questions and interesting situations.

Here are a few client issues from the past couple of months that might benefit others.

• Hospital and ambulatory surgery center in one location.

Situation: We are a hospital system that is looking to push a large amount of low-risk, high-volume surgery out of our crowded operating rooms to a freestanding ambulatory surgery center in the area. We do not seek equity but are looking for a way to maintain our identity and have our employee surgeons perform their cases in an environment that meets our high standards.

Advice: This scenario was interesting. The healthcare system also wanted to negotiate a fixed fee for its patients for various procedures. We were able to provide them an existing surgery center, with physical expansion space. The leaders were receptive to the idea. After many meetings and conversations with senior level management on both sides, we agreed on terms.

We are ending up with an immediate accommodation for the hospital surgeons, the hospital itself, their patients, and the for-profit surgery center. We agreed to build out a portion of the facility that will have its own entrance, its own logo, and its own identity.

Furthermore, we had the space for the hospital's own waiting room and reception area. Once the patients entered the surgical area, they had their own procedure rooms and recovery area, but they still were part of the "back of the house" surgery center managed by the ASC and its staff. They are not receiving any facility fee reimbursement.

There were lots of moving parts to negotiate and accommodate, but it was approved by attorneys and well worth the effort.

• Private labeling of the surgical procedure.

Situation: We were approached by and accepted clients who wanted to franchise a certain surgical procedure technique outside their successful model. The leaders wanted to build a chain of surgery centers around that concept that has made them successful, but they wanted to expand into other parts of the United States.

Advice: After many (and I do mean many) marketing meetings, demographic analyses, site visits, and new demographic studies, we found our new target location 1,500 miles away from the parent ASC to begin the franchise.

We have finished negotiations on the new space for the first of six new ASCs in the Midwest, and now we are looking for the second and third locations.

• Selling the ASC after 18 months of operations.

Situation: Anyone who develops surgery centers knows that there is a significant exit strategy for a properly developed facility. While we do not endorse an approach of "build it, and they will come," we do preach to our clients that there is a market for your surgery center, perhaps sooner than you think.

Advice: After a run of only 18 months, the owners have several entities offering multiples of earning of up to eight times to buy 80%

COMING IN FUTURE MONTHS

- Ensuring agency staff are properly screened
- Are you liable if you don't respond to staff complaints?
- Avoiding liability with hiatal hernia cases
- Ensuring adequate test-result reporting and follow-up

of the ASC. Again, this situation highlights the benefits of a well-designed ASC that is built to be sold eventually.

• Multiple ASC ventures by a hospital system.

Situation: We were engaged by leaders at a well-known New England-based hospital system who were looking for an ambulatory surgery center solution to their growing patient base, but they still wanted to maintain their market share of outpatient surgery.

Advice: After just a few months of working with the client, the leaders now have opportunities for a majority interest in one de novo surgery center at the other end of the state and the conversion of an existing off-site surgical outpatient facility to a freestanding ASC with a large new base of surgeons. They essentially are widening their market share while partnering with new surgeons and specialties.

While some of the above situations may have little to do with your particular facility, it is important to understand how dynamic outpatient surgery is becoming in the changing face of healthcare reform. Never discount anything your surgeons or department heads suggest. Who knows? You may be next! *[Earnhart & Associates is a consulting firm specializing in all aspects of outpatient surgery development and management. Earnhart & Associates can be reached at 5114 Balcones Woods Drive, Suite 307-203, Austin, TX 78759. Phone: (512) 297-7575. Fax: (512) 233-2979. Email: searnhart@earnhart.com. Web: www.earnhart.com.]* ■

Non-technical Skills Matter With Safety

Patient safety before, during, and after surgery requires an appropriately educated, committed, and empowered healthcare team, according to recommendations presented at the inaugural National Surgical Patient Safety Summit (NSPSS) in Rosemont, IL.

The goals of the Summit were to develop surgical care and surgical education curricula standards and prioritize safety research efforts.

Technical and non-technical skills are important to successfully and safely perform surgery, the NSPSS said in a released statement. The surgeon, anesthesiologist, nurses, and all supporting staff must ensure consistent use of surgical safety strategies and tools throughout surgical care, including patient-centered shared decision making and timely informed consent, standardized surgical site marking procedures, accurate surgical information transfer, integrated electronic medical records, and effective team communication and coordination, it said.

"Surgical safety improves when non-technical strategies, tools, and behaviors are combined with proficient surgical skills," said **William Robb**, MD, co-chair of NSPSS and past chair of the patient safety committee at the American Academy of Orthopaedic Surgeons. "Each member of the surgical team needs to know how to effectively communicate and appropriately adapt during an adverse situation."

Workgroups, including surgeons, anesthesiologists, and nurses, convened prior to the summit to prepare draft recommendations for all surgical team members, surgical institutions, medical and nursing schools, surgical residency and fellowship programs, and surgical credentialing organizations. The recommendations include creation and adoption of the following standardized items:

- surgical safety education programs with an assessment of competence for surgeons, residents, medical students, perioperative team members, and surgical institutions on effective communication, resilience, leadership, and teamwork;
- safety training modules (simulation-based) for the entire surgical team: doctors, nurses, anesthesiologists, surgical technicians, and physician assistants;
- "shared decision making" practices and procedures to ensure an informed and prepared surgical patient.

The NSPSS recommendations can be accessed by readers online at http://bit.ly/2bj9TCv. ■

CE/CME OBJECTIVES

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

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

SAME-DAY SURGERY

EDITORIAL ADVISORY BOARD

Consulting Editor: Mark Mayo, CASC
Executive Director, ASC Association of Illinois
ASC administrator, Chicago Surgical Clinic Arlington Heights, IL

Nurse Reviewer: Kay Ball, RN, PhD, CNOR, FAAN
Associate Professor of Nursing
Otterbein University
Westerville, OH

Physician Reviewer: Steven A. Gunderson, DO
CEO/Medical Director
Rockford (IL) Ambulatory Surgery Center

Stephen W. Earnhart, MS
President and CEO, Earnhart & Associates
Austin, TX

Ann Geier, MS, RN, CNOR, CASC
Vice President of Clinical Informatics, Surgery
SourceMedical, Wallingford, CT

John J. Goehle, MBA, CASC, CPA
Chief Operating Officer
Ambulatory Healthcare Strategies
Rochester, NY

Jane Kusler-Jensen, BSN, MBA, CNOR
Specialist master, Service operations/ healthcare providers/strategy & operations
Deloitte, Chicago

Roger Pence
President, FWI Healthcare
Edgerton, OH

Sheldon S. Sones, RPh, FASCP
President, Sheldon S. Sones & Associates
Newington, CT

Rebecca S. Twersky, MD, MPH
Chief of Anesthesia, Josie Robertson Surgery Center
Memorial Sloan Kettering Cancer Center
New York

Interested in reprints or posting an article to your company's site? There are numerous opportunities for you to leverage editorial recognition for the benefit of your brand.
Call: (800) 688.2421
Email: Reprints@AHCMedia.com

Discounts are available for group subscriptions, multiple copies, site-licenses, or electronic distribution. For pricing information, please contact our Group Account Managers:
Call: (866) 213-0844
Email: Groups@AHCMedia.com

To reproduce any part of AHC newsletters for educational purposes, contact The Copyright Clearance Center for permission:
Call: (978) 750-8400.
Email: Info@Copyright.com.

CE/CME INSTRUCTIONS

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

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

2. Scan the QR code to the right or log on to AHCMedia.com then select "My Account" to take a post-test. *First-time users must register on the site.*

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

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

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

CE/CME QUESTIONS

1. **Why might same-day surgery facilities have an increase in vulnerability to a ransomware attack, according to Ellen M. Derrico, MBA, a marketing/ market development executive in healthcare and life science technologies and an independent consultant?**

   a. The volume of patients
   b. The increased mobility of the clinicians
   c. The level of security in place
   d. All of the above

2. **If your facility's computers are infected with ransomware, you should not pay the ransom, according to a joint alert from the U.S. Department of Homeland Security and the Canadian Cyber Incident Response Centre. Why?**

   a. Paying the ransom does not guarantee the encrypted files will be released.
   b. Decrypting files does not mean the malware infection has been removed.
   c. A and B
   d. Neither A nor B

3. **The American College of Surgeons advises that scrubs and hats worn during dirty or contaminated cases should be changed prior to subsequent cases, even if not visibly soiled. What concerns has the Association of periOperative Registered Nurses raised?**

   a. Evidence shows that perioperative team members who are following standard precautions, using personal protective equipment, and conducting hand hygiene should not need to change scrubs and hats between cases.
   b. This statement may cause confusion by introducing a different standard for surgeons than for other team members.
   c. A and B
   d. None of the above

4. **What was an unexpected source of help in improving cash collections at The Cooper Health System's surgical center by 634%?**

   a. A local community college
   b. The hospital's marketing department
   c. The hospital's public relations department
   d. None of the above