### McMAHON PUBLISHING

# GENERAL SURGERY NEWS

The Independent Monthly Newspaper for the General Surgeon

GeneralSurgeryNews.com

July 2021 · Volume 48 · Number 7

Ergonomic Injuries in Surgery: A Quiet but Pervasive Problem

By VICTORIA STERN

In July 2019, Talar Tejirian, MD, had surgery to repair a herniated disk at the C5-C6 vertebrae, which provides flexibility and support to the neck. The operation went well. Aside from a stiff neck, she felt pretty good.

However, Dr. Tejirian's condition soon deteriorated during the physical rehabilitation process. Her physical therapist noted weakness in her right arm and started her on a weight lifting regimen, bypassing standard exercises to improve her range of motion.

She soon developed new, more severe pain in her right arm.

"I knew something was wrong," said Dr. Tejirian, a general surgeon at Kaiser Permanente in Los Angeles. "I had never before experienced this type of pain."

A nerve conduction test delineated the problem. The results hit her hard.

Continued on page 30

# Preventing SSIs In General Surgery

What the Data Show: An Expert's Take

By MONICA J. SMITH

Despite decades upon decades of progress in surgery, surgical site infections are still extremely common, accounting for one-fifth of all nosocomial infections.

The impact on patients ranges from trivial to deadly. And the associated costs, such as increased hospital length of stay, readmissions and admission to ICUs, can be staggering—from \$1,500 to \$5,000 per day per SSI in the United States.

Over generations, guidelines for SSI prevention have evolved as new methods are proposed, put to the test, and ultimately accepted or discarded. For now, these are the interventions known to be most beneficial in general

Continued on page 24



European Data Show Intraperitoneal Onlay Declining, Open Sublay on the Rise

By BOB KRONEMYER

Over the past decade for incisional hernia repair, there has been a significant decrease in laparoscopic intraperitoneal onlay mesh (IPOM) and a corresponding increase in open sublay mesh repair, as well as new minimally invasive techniques including mini less open sublay repair (E/MILOS), extended totally extraperitoneal repair (eTEP), and preperitoneal mesh.

The findings, which were published in *Hernia* (2021;25[2]:255-265), also showed that 10% of incisional hernias continue to be treated via an open

Continued on page 36

## Inside the Launch of The Surgical Palliative Care Society

By VICTORIA STERN

After more than a decade practicing surgery, Pringl Miller, MD, FACS, noticed a change in her patients.

Dr. Miller began seeing older and sicker patients, people who required more urgent decision making and symptom management.

"With my patients' needs shifting, I moved into acute care surgery, but I felt a gap in my ability to provide the advanced communication and supportive care my patients needed," Dr. Miller said. "As a surgeon, I always aim to mitigate suffering, but these efforts often center on technical skills, not words or touch."

Continued on page 32

## Study Suggests Which Melanoma Patients May Avoid Sentinel Node Biopsy

BY KATE O'ROURKE

Nost patients with newly diagnosed melanoma undergo a sentinel lymph node biopsy (SLNB), in which the sentinel lymph nodes are removed and examined to find whether the cancer has spread beyond the skin. Now, results from a large cohort study indicate that a proportion of stage pT1b-pT2a melanoma patients could potentially avoid SLNB. The findings were presented at the Society of Surgical Oncology 2021 International Conference on Surgical Cancer Care (abstract 59).

"The results of this large cohort study would suggest that, with the new modern treatment paradigm, a proportion of pT1b-pT2a patients could potentially avoid SLNB, since the management of these patients may remain unchanged,

Continued on page 3

#### IN THE NEWS

14 Highlights From the American Society Of Colon and Rectal Surgeons

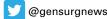
17 Tips on Being an Expert Witness

#### THE GREAT DEBATES

34 Roux-en-Y or One-Anastomosis Gastric Bypass: Which Is Better?







JULY 2021 / GENERAL SURGERY NEWS

# Why Surgeons Should Partner With Their Central Sterile Processing Department

Redefining the Relationship to Decrease Surgical Site Infections

By DAVID TAYLOR III, MSN, RN, CNOR

Over the past decade, hospitals have spent a great deal of time, resources and money to prevent surgical site infections. Properly timed antibiotics, nasal decolonization, skin antisepsis, appropriate hair removal, preoperative bathing and hand hygiene have been some of the measures taken to reduce infection rates. But one critical dimension of infection safety has received comparatively much less attention, and that is the role of the central sterile processing department (CSPD).

Central sterile processing is the first link in the chain of infection prevention. Its role is to decontaminate, clean, inspect and sterilize instrumentation for future use. However, failure to do so can introduce pathogens into the OR, increasing the risk for SSIs. The major problem is a lack of awareness of just how important this step truly is.

In U.S. hospitals, SSIs are a major problem and a significant patient safety issue. They affect a significant number of the patients and can have devastating consequences, including long-term disability (http://bit.ly/2OfAsSJ) and worse outcomes (*BMJ Open* 2016;6[2]:e007224). Most hospitals have made substantial process changes to improve intraoperative safety, but these gains are vulnerable to weaknesses in the CSPD.

### The Financial Issue

Nearly 1.5 million surgical procedures were performed in 2019. Cases declined in 2020 because of COVID-19, but experts are predicting a spike this year, with further growth in the surgical market from 2022 to 2025 (http://bit.ly/30uwTe2).

Surgical site infections are the third most expensive type of health careacquired infection (HAI), costing nearly \$21,000 per patient case. Some estimates raise that cost to \$90,000 (https://bit.ly/3cfPbVB). It's estimated that the total cost of SSIs to the U.S. health care system ranges from \$3.5 billion to \$10 billion annually (http://bit.ly/3cfPbVB).

In addition, in 2015, the Centers for Medicare & Medicaid Services began to penalize hospitals for high rates of SSIs along with other health care–acquired conditions. Because SSIs dramatically increase the risk for rehospitalization, hospitals are more vulnerable to readmission penalties (Table).

These safety and financial issues make a compelling argument for timely preventive action (*Langenbecks Arch* 

Surg 2011;396[4]:453-459). A surgeon who knows more about CSPD can have a positive effect on their own practice. When surgeons engage directly with hospital leaders to create a strong process for preventing SSIs, patient safety surely will increase.

### **Going Behind Closed Doors**

A CSPD orientation program designed to educate surgeons continued on the following page

### Table

- Of all inpatient surgery patients, 2% to 5% develop an SSI.
- Between 160,000 and 300,000 SSIs are estimated to occur every year in this country.
- On average, hospital LOS increases 7 to 11 days as a result of an SSI.
- There is a 2 to 11 times greater chance of an increase in death associated with SSIs.
- It is estimated that up to 60% of SSIs are preventable.

Sources: Infect Control Hosp Epidemiol. 2014;35(6):605-627; World J Emerg Surg. 2019;14:50.



IN THE NEWS

GENERAL SURGERY NEWS / JULY 2021

# Hospitals Urged to Strengthen Cybersecurity Systems With Attacks on the Rise

By CHRISTINA FRANGOU

As the SARS-CoV-2 virus spread globally over the last year, health care institutions became increasingly vulnerable to another kind of dangerous viral attack—this time, at the hands of cybercriminals.

During the 2021 Critical Care Congress Virtual Event of the Society of Critical Care Medicine, a panel of physicians urged attendees to take steps to protect their hospitals' cybersecurity systems, pointing out that the health care sector is now the most targeted industry by ransomware in the United States.

These attacks can significantly affect patient care, harm patients and providers and carry an enormous price tag. Medical data breaches alone cost the health care industry more than \$5.6 billion annually.

"Hacking in health care is a major problem, with estimated millions of records being breached every year in the U.S. alone," said L. Nelson Sanchez-Pinto, MD, MBI, a specialist in pediatric critical care medicine and informatics at Ann & Robert H. Lurie Children's Hospital of Chicago.

This past fall, federal agencies issued a warning that cybercriminals were targeting U.S. health care institutions. The wave of ongoing attacks was designed to lock up hospital health information systems as COVID-19 cases were spiking. Cybersecurity firm Check Point reported that ransomware attacks against American hospitals rose 71% from September to October 2020.

Cyberattacks on health systems come in three forms—phishing, malware and medical data breaches—said Dr. Sanchez-Pinto, who moderated the panel. Phishing attacks are the most common; they arrive disguised as legitimate-appearing emails that trick the recipient into opening a link or document with malware or into providing personal information.

Malware is software that users inadvertently down-load onto their devices, which infects the system with a virus. Malware can take control of a computer until a user pays a sum of money, a version known as ransomware; or it silently spies on a computer, sends data or gives access to a hacker.

Medical data breaches have become more frequent in recent years; hackers steal medical records and sell them on the dark web. They can fetch up to \$1,000 per patient because of the breadth of information in medical records. Information contained in these files can be used for fraud or identity theft, as well as blackmail or extortion. Provider data can also be accessed and used for fraudulent insurance claims or prescription drug fraud.

Dr. Sanchez-Pinto said physicians and their colleagues must create a culture focused on cybersecurity,



Erie County Medical Center, the Buffalo trauma center attacked by a variant of ransomware named SamSam.

Credit: D-Day/Wikimedia Commons

although it means some tasks require more time.

"Taking extra security steps online can be annoying because it can seem like they are slowing our workflow, but we owe it to our patients to be safe with their data because it's extremely vulnerable," he said.

On April 9, 2017, the Level I trauma center at the University of Buffalo was hit by a variant of ransomware named SamSam. The attack shut down the hospital's HIS, including all electronic clinical applications, billing and scheduling services, and communication tools. The hospital decided not to pay the ransom and turned to old-fashioned paper charts and face-to-face communication for two months while the HIS was restored.

In that time, staff lost access to the electronic medical record (EMR), the picture-archiving and communication system, and even the internet.

Physicians could access patients' historical data,

including medical records and imaging, through HealtheLink, an electronic clinical information exchange among hospitals in Western New York. Otherwise, patient information was communicated only in writing, by phone and in person.

W. Alan Guo, MD, an acute care surgeon and a surgical intensivist at the University of Buffalo, said trainees struggled with the abrupt switch to a paper-based system as they came to medicine in the era of the EMR.

In a study published in 2018, Dr. Guo and his colleagues reported that residents were very stressed by the lack of online resources in the aftermath of the attack (*J Surg Res* 2018;232:389-397). Some surgical residents said they had less hands-on experience in the OR because limited imaging made cases more difficult.

He urged hospitals to treat ransomware attacks like other disasters and prepare for them as part of disaster planning. Training in paper-based documentation should be included as part of hospital in-service and the graduate medical education curriculum, he said.

"Everything is digital now. So, younger generations need to learn about paper-based documentation in case something happens, because the cyberattack rate is getting higher and higher in this world."

During the pandemic, health systems have become more dependent on smart devices and telemedicine. This reliance makes hospitals more vulnerable to major attacks, according to Piyush Mathur, MD, a staff anesthesiologist and critical care physician at Cleveland Clinic in Cleveland. He chairs Cleveland Clinic's Anesthesiology Institute compliance committee.

"We need to understand that despite telemedicine providing access to a lot of different patient care areas, it has vulnerabilities and we need to be prepared for that," he said.

Telemedicine systems rely on a network of products that are built in one country, used in another and perhaps serviced in yet another. These systems can be accessed by a global network of people working at multiple points in the chain, including human resources programs, audiovisual intersections and even IV pumps at the bedside.

"These, across the entire nation, are all vulnerable to attack," Dr. Mathur said.

### **CSPD**

continued from the previous page

represents a low-cost, high-impact opportunity that not only drives the alignment between key customers of the OR, but can improve safety and efficiency

Individual and small group tours are an important start, and can give the surgeon a general overview of the inner workings of the CSPD and how it may affect their practice. To increase the return on investment, a more robust program can be created by taking this concept further and allowing the leaders to present at a Department of Surgery meeting. Once established, the leaders can grow the orientation program and combine it with

the introduction of a quarterly surgeon satisfaction survey.

Program components can consist of the following:

- Walk through each area of the department.
- Detail the time it takes for accomplishing each step.
- Explain the equipment used in the process.
- Introduce surgeons to the staff responsible for their instruments.

### What's There to Learn?

Efficient turnover of instrumentation can help ensure the surgical team has the necessary equipment to perform its procedures. However, far too often when instrumentation is missing, CSPD gets

the blame. When surgeons have a better understanding of the department and its inner workings, they can begin to truly understand where the issues lie.

First and foremost, knowing your set inventory is critical. When a surgeon schedules five procedures for the day and the hospital has only three instrument sets, delays are inevitable. Most organizations require loaner instrumentation to arrive 24 to 48 hours before the surgery to ensure it has been properly inventoried, inspected, decontaminated, reassembled, sterilized and packaged. Also important to note, it takes on average three to four hours for an instrument set to be proper processed, and that's a low estimate. In this scenario, it's called an instrument turnover.

So, when the surgeon asks why their case is delayed and the circulating nurse says the instruments are not ready, it's easy to see why the CSPD would be blamed. The truth is the department most likely had requested additional instrumentation to improve processes; however, due to the high cost of instrumentation, the request probably was denied.

Finally, consistent turnover of instrumentation can result in corners being cut and a greater possibility that something was missed, which can have devastating consequences.

—David L. Taylor III, MSN, RN, CNOR, is the principal of Resolute Advisory Group LLC, a health care consulting firm in San Antonio.