HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE FOR MORE THAN THREE DECADES

INSIDE

Nurse sues hospital for suspension 53

Ransomware attacks on the rise. 54

Liability possible from scope recall. 56

Insurance companies are looking at cyber risk. 57

Stryker offers sponge indemnity 57

Are EHRs linked to higher rates of adverse events? 58

Enclosed in this issue:

- *HIPAA Regulatory Alert*
- *Legal Review & Commentary*
- *2016 Reader Survey*

AHC Media

MAY 2016 Vol. 38, No. 5; p. 49-60

Can alarm fatigue be conquered? Yes, say hospitals cutting the noise

The problem of alarm fatigue has gained attention in recent years, with evidence showing that it can threaten patient safety. Now hospitals are finding ways to effectively address the problem by minimizing the number of alarms and prioritizing the rest, and they also are finding that something as simple as a trash can lid can play a role in alarm fatigue.

Alarm fatigue has risen to the level of a recognized safety risk that must be addressed. The Joint Commission (TJC) found 98 alarm-related instances of patient harm, including 80 deaths and 13 cases of permanent disability between January 2009 and June 2012. As of January 2016, TJC's National Patient Safety Goals (NPSGs) mandate that hospitals take definitive steps to implement policies and procedures to safely reduce and prioritize the number of primary and secondary alarms. The ECRI Institute ranked alarm proliferation as the second top technology hazard in 2016, and an investigation by the *The Boston Globe* found more than 200 deaths nationally related to alarm problems. *(To access the TJC report, go to http://bit.ly/1PI4ilQ. You can access the NPSG related to alarm fatigue at http://bit.ly/1qYEnL6. Readers can access ECRI's technology hazards at http://bit.ly/1WQJIUM. Access the report from* The Boston Globe *online at http://bit.ly/1MWEX7Q.)*

"WE WANTED TO PUT THE RIGHT ALARM WITH THE RIGHT PERSON AT THE RIGHT TIME."

— CONNIE DILLS, MBA, RRT, RPFT, HOSPITAL FOR SPECIAL CARE

Several hospitals are reporting success with their efforts to reduce alarm fatigue. Boston Medical Center recently reported that its analysis showed the vast majority of warning alarms at the hospital don't need an audible signal, so the hospital

Financial Disclosure: Author Greg Freeman, Executive Editor Joy Daughtery Dickinson, and Nurse Planner Maureen Archambault report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study. Arnold Mackles, MD, MBA, LHRM, physician reviewer, discloses that he is an author and advisory board member for The Sullivan Group and that he is owner, stockholder, presenter, author, and consultant for Innovative Healthcare Compliance Group.

HEALTHCARE RISK MANAGEMENT™

Healthcare Risk Management™, ISSN 1081-6534, including HRM Legal Review & Commentary™ 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: Healthcare Risk Management, P.O. Box 550669, Atlanta, GA 30355

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

SUBSCRIPTION PRICES: USA, Print: 1 year (12 issues) with free CE nursing contact hours and free *AMA PRA Category 1 Credits*™, $519. Add $19.99 for shipping & handling. Online only, single user: 1 year with free CE nursing contact hours and free AMA PRA Category 1 Credits™, $469. Outside USA, add $30 per year, total prepaid in USA 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 $87 each. (GST registration number R128870672.)

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 1.5 nursing contact hours using a 60-minute contact hour. Provider approved by the California Board of Registered Nursing, Provider #CEP14749, for 1.5 Contact Hours.

AHC Media designates this enduring material for a maximum of 1.5 *AMA PRA Category 1 Credits*™. Physicians should claim only credit commensurate with the extent of their participation in an activity.

Healthcare Risk Management™ is intended for risk managers, healthcare administrators, healthcare legal counsel, and physicians. This activity is valid 24 months from the date of publication.

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

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

EDITORIAL QUESTIONS
Questions or comments?
Call Editor **Greg Freeman**, (770) 998-8455.

decided it was safe to switch them off. At the same time, the hospital also upgraded some low-level warning alarms to a higher level that signifies a crisis. Boston Medical also gave nurses authority to change alarm settings to account for the differences among patients. As a result, just one division of the hospital went from 90,000 alarms a week to 10,000. *(The hospital's experience with addressing alarm fatigue is described in the* Journal of Cardiovascular Nursing, *which readers can access online at http://bit.ly/1RPVulq.)*

Texas Children's Hospital (TCH) in Houston addressed alarm fatigue with multiple strategies. Hospital leaders wanted to create a safer patient environment by making alarms more meaningful and useful to clinicians, explains **Jennifer Sander**s, MSN, RN, NEA-BC, director of clinical support operations at the hospital. Initial efforts focused on gathering data to quantify what clinicians knew anecdotally: that there were too many alarms going off too often, and they had a detrimental effect on patient care. TCH worked with an outside clinical decision technology vendor, Medical Informatics Corporation in Houston, TX, to develop an alarm dashboard that provided a patient-level analytics platform the care team could use to make decisions about alarm settings. *(See the story in this issue for an example of patient alarm data.)*

The hospital also formed a multi-disciplinary team with membership from the medical staff, nursing staff, clinical informatics, biomedical engineering, information services, and the vendor. TCH chose the Progressive Care Unit (PCU), a step-down intensive care unit, as an early adopter unit because it was known anecdotally to have a high number of alarms. The team began collecting data from the electronic medical record, cardiac monitoring system, and nurse staff assignments.

The team made recommendations based on a 53-day data analysis, which included an onsite environmental analysis, multiple staff interviews, and a comprehensive analysis of the alarm and patient data collected in the PCU. Based on these findings, the team decided to use a Plan-Do-Study-Act (PDSA) approach, a four-stage problem-solving model used for improving a process or carrying out change. The hospital started with simple changes and progressed to the introduction of patient-specific alarm dashboards. For example, some of the first changes involved simple environmental improvements such as changing trash and linen bins so that they would not make as much noise.

"We realized that every time a nurse would wash her hands and throw the paper towel away in the trash bin, the lid would make a very loud noise, and all the patient alarms would go off because they were startled and their heart rates went up," Sanders explains. "The simple fix was putting silent closing lids on the

EXECUTIVE SUMMARY

The Joint Commission's National Patient Safety Goals require hospitals to address alarm fatigue.

- At least 80 deaths have been tied to the problem.
- One hospital division reduced alarms from 90,000 per week to 10,000.

trash cans, and that alone produced an almost 3% reduction in alarms on those units."

Alarm threshold changed

The team went on to adopt a new alarm threshold for low peripheral capillary oxygen saturation (SpO2), an estimate of the amount of oxygen in the blood. The standard alarm threshold was changed from 93% to 90%, though physicians can set it differently for individual patients. This change in the standard threshold resulted in a 10% reduction in SpO2 alarms per bed per day, a 13% reduction SpO2 as a percentage of total alarms in the unit, and a 15% reduction in SpO2 alarms that lasted fewer than 10 seconds, also known as chattering alarms and considered one of the most annoying.

The next step was educating the staff about alarm management and the proper way to use silence and suspend functions. Nursing education resulted in an additional 11% reduction in SpO2 alarms per bed per day.

Finally TCH introduced the patient-specific dashboards that can be reviewed during rounds, which enabled physicians to engage in the alarm management improvement process and evaluate alarm settings for specific high alarming patients. The process takes an average of less than two minutes per patient during rounds, Sanders says. Presented graphically, the patient dashboard shows, for example, that the patient experienced 122 SpO2 alarms in the past 24 hours. This information means that the patient's "time in alarm" or amount of time alarms sounded in the room was 52 minutes and 27 seconds over the last 24 hours. The data also show that compared to the prior day, the alarm count is greatly reduced. A plot shows alarms aggregated by time of day. Currently, the patient's SpO2 limit is set to 90%, but this patient's 95% confidence limit of observed vitals are between 81% and 96%. A table also provides data to the care team regarding the potential impact of changing the patient's SpO2 threshold.

"They have real-time conversations about this particular patient and how the alarms are sounding," Sanders explains. "They can discuss whether the patient really was decompensating and needed intervention, or whether we need to change the alarm parameters to avoid nuisance alarms."

Rather than focusing on alarm fatigue as a technology problem or a nursing problem, the multidisciplinary team considered it a patient care issue and sought ways to improve the patient experience, she says. Assessing the data from different perspectives was important, Sanders says. The unit level data showing the alarms by bed can help identify the patients frequently in alarm status, and the nurse-level information depicts the alarm load by nurse, which allows nursing leaders to review patient assignments for appropriateness of total alarm volume by staff nurse. The patient view shows the alarms by patient for the past 24 hours and provides data and recommendations on changes to alarm limits to reduce alarm fatigue.

"This was a project that brought almost instant gratification," Sanders says. "You could look at the data, make a change, and almost immediately see a change in the alarms and the noise on the unit."

Alarms cause fatigue

The Hospital for Special Care (HSC) in New Britain, CT, also has taken aim at alarm fatigue and reduced ventilator alarms by 80%, says **Donna M. Reinholdt**, MHL, MM, RN, LNC, director of corporate risk management and compliance.

The hospital formed an alarm committee a year in advance of TJC's implementation of the alarm safety NPSG. It included the chief of pulmonary medicine, leaders from respiratory medicine, and respiratory therapists, who are responsible for responding to most alarms. The committee identified all high-risk clinical alarms, assessed device-specific alarms, and prioritized both the devices and specific alarms on each device. The goal was to differentiate which alarms were immediately actionable from those that were non-emergent, Reinholdt explains.

"The committee continues to meet on a regular basis and reviews any risk-related concerns regarding alarm device volume and audibility," Reinholdt says. "The committee utilizes a true risk management strategy in coping with potential alarm device fatigue by implementing monitors that measure response time and volume, as in the number of alarm conditions occurring."

Most of the patient population at HSC is mechanically ventilated, so the threat of alarm fatigue stemmed primarily from those devices, Reinholdt notes. The Respiratory Therapy Department at HSC manages more than 100 ventilators, each with its own set of alarms, at patients' bedsides across the hospital. In addition to the ventilator alarms, staff still had to deal with alarms from the usual mix of devices found in any hospital, such as pumps and physiological monitors.

For many years the number of ventilators and the complicated layout of the units forced the hospital's respiratory therapists to spend much of their shifts racing from room to room responding to hundreds of non-actionable alarms, says **Connie**

Dills, MBA, RRT, RPFT, respiratory practice manager at HSC. Most of the alarms were for events that, while noteworthy, did not require immediate intervention, she explains. Not only did the repeated alarms distract staff and take them away from other duties, but the noise also disturbed patients who were trying to recover.

"Alarm fatigue was a huge problem for us," Dills says. "A lot of the fatigue was from everyone getting every alarm all the time. We wanted to put the right alarm with the right person at the right time."

Alarms prioritized

With mechanical ventilation, the most critical alarm is for low exhaled minute volume, which indicates too little gas exhaled from a person's lungs per minute.

That alarm can mean the patient is not being ventilated because there is a mechanical malfunction, a leak, or some other problem, Dills explains. However, the ventilators also can alert therapists to conditions such as high pressures and low respiratory rates, which are not critical but can lead to low exhaled minute volume if they persist. Those alarms could be triggered by something benign such as the patient coughing or talking and did not indicate a persistent condition that would become critical, Dills explains.

"In most cases there was no need to respond, and in fact, there often was someone with the patient, and that's why they were talking and setting off that alarm," Dills says. "But if you don't have volume coming back to the ventilator, that's a big indicator that they're not being ventilated, and someone needs to respond right away."

One of the first improvements was to route ventilator alarms through pagers to the specific respiratory therapist assigned to each patient. The hospital also changed how alarms were transmitted.

The critical alarms, such as low exhaled minute volume and patient disconnect, are routed to the handheld paging system as well as the overhead alarm system so a therapist can respond promptly. The non-critical alarms — those for conditions that are not immediately threatening — do not go through the handheld paging system, and they are not broadcast on the unit. The computer system tracks those alarms, however, and a non-critical alarm that does not self-correct will result in an actionable/critical alarm that will go into the paging system and overhead system.

That change greatly reduced the cacophony of alarms in the hospital, Dills says. To enable the alarm filtering and prioritization, HSC used the Bernoulli One software system that provides continuous surveillance and alarm monitoring, manufactured by Bernoulli, a company based in Milford, CT, that provides device and software products for healthcare facilities. *(In addition to Medical Informatics and Bernoulli, products for medical device integration are available from other companies such as Capsule in Andover, MA, Excel Medical in Jupiter, FL, and Iatric Systems in Uxbridge, MA.)*

The system first was implemented in the Pediatric Unit, which has the most complex layout, making it difficult for clinical staff to move quickly from patient to patient. The unit utilizes three types of ventilators from different manufacturers, so a vendor-neutral approach was critical, Dills explains.

The software system also allowed the hospital to provide networked laptop and desktop computers with scrolling message bars at key locations. These computer stations provide the respiratory therapists with access to data and alarms from all ventilated patients so that when they receive alarms on their pagers, they quickly can assess the patient's status without having to go to the bedside immediately.

Real-time data from the networked system also enabled the respiratory therapists and the alarm committee to start identifying non-actionable alarms that could be adjusted or eliminated entirely, which contributed to the 80% reduction in ventilator alarms in the Pediatric Unit. After successful implementation in the Pediatric Unit, the system was expanded to the Respiratory Care and Respiratory Step-Down units as well, with similar results.

The change in alarm procedures was welcomed by the respiratory therapists and nursing staff, Dills says. The units are much quieter than before the alarm fatigue initiative. Rather than worrying that downgrading some alarms would threaten patient safety, the respiratory therapists are more confident that they know when to respond quickly to an emergency, she says.

"We recently had a server upgrade that took the system down for a while, and the therapists were just beside themselves that they were going to miss an alarm," Dills says. "They know now that they can trust the alarms and really respond when necessary. Previously there were so many alarms that nurses and therapists sometimes stopped hearing them, and that was scary."

SOURCES

- **Connie Dills**, MBA, RRT, RPFT, Respiratory Practice Manager, Hospital for Special Care, New Britain, CT. Telephone: (860) 827-

1958, Ext. 5706. Email: cdills@hfsc.org.
- **Donna M. Reinholdt**, MHL, MM, RN, LNC, Director of Corporate Risk Management and Compliance, Hospital for Special Care, New Britain, CT. Telephone: (860) 827-1958, Ext. 4330. Email: dreinholdt@hfsc.org.
- **Jennifer Sanders**, MSN, RN, NEA-BC, Director of Clinical Support Operations, Texas Children's Hospital, Houston. Telephone: (832) 826-5253. Email: jlsander@texaschildrens.org. ■

Nurse sues hospital for suspension related to suicidal comments

When do an employee's personal troubles threaten patient safety and justify limiting work duties? A certified registered nurse anesthetist (CRNA) recently sued a hospital after it put her on sick leave and demanded a psychiatrist approve her return to work, which was prompted by her statements suggesting suicidal thoughts and the concerns voiced by her coworkers.

The case went to an appeals court after initially being dismissed and, in the process, raised questions about how hospitals can protect patient safety without treating an employee unfairly. Peggy J. Barnum, CRNA, sued Ohio State University Medical Center (OSUMC) for putting her on sick leave and demanding that she first secure a fit-for-duty recommendation from a psychiatrist, and then sign a release letting the hospital talk to the psychiatrist, before it would agree to reinstate her. Hospital officials claimed that she had expressed suicidal thoughts at work and was so distracted that she could no longer care for patients safely. Barnum's lawsuit accused the hospital of retaliation and of violating various First Amendment and disability-related rights. An appeals court recently sided with the hospital and affirmed a lower court's dismissal of her claims.

Barnum was out of work for the next 13 months, says her lawyer **Daniel H. Klos**, JD, of Columbus, OH. He says the dispute began when Barnum was overheard by another CRNA saying something to the effect of, "Maybe I'd be better off if I wasn't here. Maybe I should just put a gun to my head. Maybe I should just not be here." Barnum was having marriage difficulties and other personal problems at the time. An anesthesiologist also reported concerns to administration and said he and several other surgeons and anesthesiologists thought Barnum was unable to concentrate on patients. During one surgery, the surgeon had to ask Barnum at least twice to raise a patient's table. When she finally replied, the anesthesiologist claimed, Barnum said, "I'm worthless. What good does it do or what difference does it make? Why should I even be here? Maybe I should do everybody a favor and not be around." The head CRNA and other CRNAs also reported their concerns.

Hospital administrators instructed Barnum to report to the emergency department (ED) for a suicide risk evaluation, which she did. A physician there released her and said she was not a threat to herself but that he could not determine whether she was fit for duty, Klos says. Her work history and reviews at the hospital were exemplary, Klos says. Nevertheless, the hospital put Barnum on sick leave and demanded a psychiatrist report saying she was fit for duty. Hospital officials also required Barnum to give her permission for them to talk to the psychiatrist and for the psychiatrist to release information about her. She produced the fit-for-duty report four months later, but the hospital still refused to reinstate her for another nine months, her lawyer says.

The Americans with Disabilities Act (ADA) requires an employer to provide reasonable accommodation to an employee with a disability, but Klos says OSUMC refused to accommodate her even as its leaders insisted she was disabled with suicidal thoughts. However, the appeals court ruled that requiring Barnum to undergo a psychiatric examination

EXECUTIVE SUMMARY

A nurse sued a hospital for putting her on sick leave in response to her comments about being suicidal and concerns expressed by colleagues. The hospital kept her out of work for 13 months.
- An appeals court sided with the hospital.
- The nurse's lawyer says the hospital overreacted.
- The hospital's lawyer claimed that there was reason to doubt the nurse's ability to work.

did not amount to labeling her as disabled and that it was reasonable for OSUMC to insist that it be allowed to talk to her psychiatrist before reinstating her.

Hospital overreacted?

Klos says the case raises questions about an employer's ability to take actions such as requiring a psychological evaluation and suspending, reassigning, or dismissing an employee for statements that are unusual but have no bearing on the person's duties in the workplace. Any statement Barnum made implying suicidal thoughts were taken too seriously and did not affect her performance, he says.

"They had one instance of one hearsay complaint by an employee who said, 'I think she could use some time off for herself,'" Klos says. "Those are the exact facts that existed on the day she was ordered to the ED. That is not enough to justify an egregious violation of her privacy and her rights under the ADA."

A spokesman for OSUMC declined to comment on the case because the litigation is pending, but in the oral arguments before the appeals court, **Rory Callahan**, JD, an attorney with the Ohio attorney general's office, represented OSUMC and argued that the hospital's actions were in response to more than just the comments overheard at work. The concerns of her coworkers raised legitimate questions about her ability to perform her duties, he said. An appeals court judge questioned why those concerns were not documented. Callahan responded that there was an incident reporting system at OSUMC, but comments were not documented.

"I would argue that OSU doesn't have to wait for an accident to occur before they can report something," Callahan argued.

Even though the hospital won the appeal, Klos notes that it spent significant time and money on the defense. He suggests that healthcare facilities must be far more cautious about responding to comments overheard in the workplace and that significant evidence is needed before intruding so significantly in an employee's personal life and career.

"If a hospital reacted this way to every emotional comment at work from someone who's going through a divorce, the Spanish Inquisition would be a cakewalk in comparison," Klos says. "They had no documents to support this. They probably have six different records to document giving out an aspirin, but they have no incident reports, nothing written, just anecdotal reports that aren't even documented, and they say that justifies sending her for a psych evaluation."

The court records are available online at http://1.usa.gov/1TlsJft. The audio of the oral arguments before the appeals court is available online at http://1.usa.gov/1RNIwhQ.

SOURCE

- **Daniel H. Klos,** JD, Columbus, OH. Email: klosdhesq@aol.com. ■

Ransomware attacks are on the rise, and hackers are getting better

On the heels of four incidents in which hospitals were hit with ransomware attacks, the U.S. Department of Homeland Security and the Canadian Cyber Incident Response Centre jointly released an alert that warns about several prominent ransomware variants that have emerged over the past few years, including Symantec, Xorist, CryptorBit, CryptoLocker, Samas, and Locky.

Ransomware attacks involve hackers seizing control of a hospital's computer system and records, then demanding payment for the encryption key or regaining control. Methodist Hospital in Henderson, KY; Chino Valley Medical Center in Chino, CA; and Desert Valley Hospital in Victorville, CA, were all the victims of ransomware attacks recently, but none is believed to

EXECUTIVE SUMMARY

Four hospitals recently were hit with ransomware attacks, in which hackers seize control of a computer system and demand money for its release. One of the hospitals paid the ransom.

- Ransomware attacks are increasing.
- Hackers are becoming more proficient, and hospital IT programs are not keeping up.
- Authorities discourage victims from paying the ransom.

have paid the ransom. Instead, the hospitals regained control through other means. Kentucky Methodist Hospital was forced to shut down all of its desktop computers and activate a back-up system, declaring "an internal state of emergency." The hospital released a statement saying no patient data or care had been affected.

Hollywood Presbyterian Medical Center in Los Angeles paid $17,000 in bitcoin, which is a type of digital currency, to regain access to its computer files.

"The malware locks systems by encrypting files and demanding ransom to obtain the decryption key," President and CEO **Allen Stefanek** said in a statement issued after the payment. "The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key. In the best interest of restoring normal operations, we did this."

The hospital was hit by one of most common ransomware types called Locky, which usually arrives in a spam email with an attached document advising readers to enable macros "if the data encoding is incorrect." Once the malware is downloaded, it sends a message to desktops with instructions about how users can pay to have files unlocked.

The U.S. and Canadian governments recommend users do not pay the ransom if they are hit with a ransomware attack, and they say providing payment does not guarantee the files will be released.

"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. In addition, decrypting files does not mean the malware infection itself has been removed," according to the alert. *(The alert is available to readers online at http://1.usa.gov/1RBQRWD.)*

More attacks to come

Hospitals can expect more ransomware attacks, says **Ellen M. Derrico**, MBA, CHM, senior director of global product marketing for healthcare and life sciences at RES, a company in Radnor, PA, that provides digital security services.

"It's not if, it's when. Ransomware attacks have increased twofold in the past six months, and I hear about new attacks every day," Derrico says.

> "IT'S NOT IF, IT'S WHEN. RANSOMWARE ATTACKS HAVE INCREASED TWOFOLD IN THE PAST SIX MONTHS, AND I HEAR ABOUT NEW ATTACKS EVERY DAY."

Paying the ransom happens a lot more often than many may think, she says. The Hollywood Presbyterian incident may be the first time it's happened in healthcare — at least to such a dramatic and public extent — but it most certainly has happened elsewhere, she says. Victims often have no choice because the hackers are getting better all the time.

Derrico says she personally knows of dozens of organizations that have been hacked in a similar manner. But until now, most were able to regain control without paying the ransom, she says. It required time, effort, and resources, and it caused lots of disruption, but in most cases the IT professionals were up to the task.

"Today, increasingly, IT is not up to task," she says. "The hackers are getting so good, sometimes paying up is actually the better choice."

Patient safety threat

Derrico notes that ransomware attacks directly threaten patient safety. Hollywood Presbyterian 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.

The financial cost to a hospital could be significant, but a ransomware attack also damages the hospital's reputation unless it can show that it had a response plan and quickly recovered without paying the ransom, Derrico says.

"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."

SOURCE

Ellen M. Derrico, MBA, Senior Director, of Global Product Marketing for Healthcare and Life Sciences, RES, Radnor, PA. Telephone: (610) 991-3076. ■

Healthcare facilities could face liability from recall of duodenoscope

Healthcare facilities and providers face potential liability related to the use of a scope that has been recalled and is the subject of lawsuits against the manufacturer.

Olympus Corp., manufacturer of about 85% of medical scopes used in the United States, recently announced a recall and redesign of its controversial duodenoscope, which has been linked to the spread of deadly infections. The announcement came in the wake of a U.S. Senate committee report that found that the medical device manufacturer knew about a design flaw in the device for years without taking action.

Hospitals, surgery centers, and surgeons are unlikely to face strict liability related to the questionable scopes because they did not sell the scope to the patient but, rather, provided a service using the scope, says **Amy Alderfer**, JD, an attorney with the law firm of Cozen O'Connor in Los Angeles. However, there could be liability if plaintiffs allege that the facility or provider did not follow the manufacturer's cleaning guidelines, she says.

Olympus updated its cleaning guidelines once concerns were raised about the scope, so a hospital or surgery center could be held liable for not following the updated procedures, Alderfer says.

"There were very rigorous requirements for how the scope had to be cleaned," she says. "You want to see documentation that you were very strictly following those cleaning requirements so that you are not exposed to a negligence action by a plaintiff."

> ... A U.S. SENATE COMMITTEE ... FOUND THAT THE MEDICAL DEVICE MANUFACTURER KNEW ABOUT A DESIGN FLAW IN THE DEVICE FOR YEARS WITHOUT TAKING ACTION.

Another potential area of exposure involves adverse event reporting and patient notification. The Senate committee report noted a lack of adverse event reports and patient notifications from hospitals. The widow of a Seattle area man who died after contracting a drug-resistant infection at Virginia Mason Medical Center in Seattle is suing the hospital and Olympus, and part of the case hinges on allegations that the hospital did not tell his family that the infection came from an Olympus duodenoscope. Virginia Mason recently began notifying patients and family members who were part of an outbreak that infected 32 people between 2012 and 2014.

Facilities and providers that used the recalled scope should assess their liability exposure by determining how well they followed the updated cleaning guidelines, whether they reported adverse events, and whether they properly notified patients involved with any scope-related infections, Alderfer suggests. *(For more on how hospitals are responding to the potential liability associated with the scope recall, see "Hospital joins plaintiff in suing scope maker," Healthcare Risk Management, July 2015, at http://bit.ly/1qln3GU.)*

"This also is an important learning opportunity, even if you determine that you have little or no exposure related to this particular recall," Alderfer says. "There are lessons here regarding the importance of following a manufacturer's infection control guidelines and also the liability that can arise when you fail to notify patients promptly. Even when the injury is the result more of the device than the service the hospital provided, neglecting patient notification is one of the most likely ways you will be involved in messy litigation."

EXECUTIVE SUMMARY

Healthcare providers could face liability related to the recall of an Olympus duodenoscope. Failure to properly clean the device or report adverse events could create liability exposure.

- Hospitals are unlikely to be involved in strict liability claims.
- The manufacturer updated its cleaning guidelines after safety concerns.
- Failure to report scope-related infections also creates liability.

SOURCE

- **Amy Alderfer,** JD, Attorney, Cozen O'Connor, Los Angeles. Telephone: (213) 892-7941. Email: aalderfer@cozen.com. ■

Insurance firms looking to evaluate cyber risk

Insurance underwriters are increasingly investigating ways to evaluate cyber risks and help healthcare organizations ensure health information systems and services are adequately protected, according to recent testimony from **Daniel Nutkis**, CEO of The Health Information Trust Alliance (HITRUST), healthcare leaders and security experts based in Frisco, TX.

Nutkis testified at a Homeland Security Committee hearing in front of the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. HITRUST offers guidance on cyber security and compliance. *(For resources, go to www.hitrustalliance.net and select the "downloads" tab on the upper right.)* The purpose of the hearing was to examine the role of cyber insurance in risk management, to try to determine what the government can do to further the efforts of the cyber insurance market, and to encourage companies to better evaluate risk and lower premiums for customers to reinvest in further protecting patients.

During the testimony, Nutkis asserted that, along with reducing the overall financial impact of cyber-related incidents or breaches on an organization, cyber insurance and cyber insurance underwriters can play a key role in supporting an organization's overall risk management strategy and help provide for the "adequate protection" of patient information. After analyzing the benefits of an underwriting program leveraging a robust risk management framework, HITRUST began educating underwriters on a cybersecurity assessment methodology that would provide the industry with consistent, repeatable, reliable, and precise estimates of cyber-related risk.

The testimony added that Allied World U.S., the first company to offer preferred terms and conditions based on meeting the HITRUST certification standards, conducted a review and analysis that determined that organizations that had obtained a HITRUST certification generally posed lower cyber-related risks than those organizations that have not. The comprehensiveness and improved risk reporting enabled by the HITRUST scores in place of many of the standard information security application questions create a more streamlined and consistent application process, Nutkis testified.

Nutkis told the Subcommittee that there are discussions with five other cyber underwriters regarding leveraging this approach, with an expectation that two more will be participating by midyear. ■

Stryker offers $5 million indemnity for lost sponges

Stryker Corp. in Kalamazoo, MI, recently announced the availability of SurgiCount Promise, a risk-sharing program that protects a hospital's investment in the SurgiCount Safety-Sponge System with up to $5 million in product-liability indemnification and a rebate of the cost of implementing SurgiCount.

Despite efforts by hospitals nationwide to improve patient safety, retained surgical items (RSIs) continue to be the number one reported surgical "never event," and 69% of all RSIs are retained surgical sponges. There are an estimated 11 incidents of surgical sponges being left inside patients every day in the United States, which results in unnecessary pain and suffering and an average annual cost of $2.4 billion to the healthcare system, Stryker notes. Numerous independent organizations, including The Joint Commission, the Association of periOperative Registered Nurses, and the American College of Surgeons, recommend the use of adjunct technology to supplement manual sponge counting to reduce the risk of retained sponges.

Dylan Crotty, vice president and general manager of Stryker Surgical, announced the new program, saying, "The SurgiCount Promise gives participating hospitals complete confidence to invest in patient safety by shifting product-cost risk to us."

The SurgiCount Safety-Sponge System uses uniquely identified sponges and towels to provide a precise, real-time count of the items. Unlike the traditional manual count procedure, which relies on a whiteboard that is erased at the end of a procedure, a record of the SurgiCount-verified correct count is maintained in the hospital's software so that surgeons, nurses, and administrators have a permanent record of the verified count.

Stryker offers qualifying facilities two layers of financial protection. If a patient experiences a retained sponge during a surgery in which SurgiCount was used as directed, SurgiCount will pay up to $5 million in legal costs for the provider and refund the participating facility's incremental

cost of implementing SurgiCount over its previous sponge spending for up to three years.

The SurgiCount system is in use in more than 480 hospitals nationwide, Stryker reports. Nearly 170 million SurgiCount Safety Sponges have been used in more than 9 million procedures over the past five years, and the company claims the system has never failed to identify a retained sponge. ■

AHRQ: EHRs associated with fewer adverse events

Cardiovascular, pneumonia, and surgery patients exposed to fully electronic health records were less likely to experience in-hospital adverse events, according to a new study from the Agency for Healthcare Research and Quality (AHRQ).

Using 2012 and 2013 Medicare Patient Safety Monitoring System data, researchers examined the association of hospitals' electronic health records adoption and occurrence rates of in-hospital adverse events. The primary outcomes evaluated were the occurrence rates of 21 in-hospital adverse events, classified by four clinical domains: hospital-acquired infections, adverse drug events, general events (such as falls and pressure ulcers), and post-procedural events. Among the more than 45,000 patients who were at risk for nearly 350,000 adverse events in the study sample, 13% were exposed to fully electronic health records.

Among all study patients, the occurrence rate of adverse events was 2.3% (7,820 adverse events). Patients exposed to fully electronic health records, however, had 17–30% lower odds of any adverse event. An abstract of the study is available online at http://1.usa.gov/1KOL4j4. ■

Summit focus: Efforts to improve diagnosis accuracy

Responding to the 2015 *Improving Diagnosis in Healthcare* report from the Institute of Medicine (IOM) that placed a public spotlight on the issue of diagnostic accuracy, the American Board of Medical Specialties (ABMS) and the National Patient Safety Foundation (NPSF) recently brought together experts to address the issue.

According to the IOM report, diagnostic errors play a role in roughly 10% of patient deaths and 6-17% of adverse events in hospital settings. Defining diagnostic error as "the failure to (a) establish an accurate and timely explanation of the patient's health problem(s) or (b) communicate that explanation to the patient," the IOM report characterizes diagnosis as a process in which every patient and healthcare professional must be an active and engaged participant.

The ABMS and NPSF focused attention on diagnostic errors with the Summit on Certification & Diagnostic Accuracy, which brought together experts from many fields to explore the cause of diagnostic error; the competencies essential to quality patient care; and the ways that certification, by engaging physicians in assessment and learning, can further reduce the risk of error. The summit report includes the presentations, discussions, and insights on how healthcare professionals can work together to improve diagnostic accuracy. The report is available to readers online at http://tinyurl.com/jkwhtqu. ■

Permitted uses of PHI explained in ONC blog

The Office of the National Coordinator for Health Information Technology (ONC) has launched a new four-part blog series to explain how the Health Insurance Portability and Accountability Act (HIPAA) not only protects personal health information from misuse, but also allows health information to be accessed when it is needed for patient care.

ONC released two new fact sheets with examples of when electronic protected health information

COMING IN FUTURE MONTHS

- Quick settlement not always best
- Increasing enforcement of HIPAA
- Inaccurate info from dementia patients
- Best practices for safety huddle

(PHI) can be exchanged without a patient's authorization under certain conditions. HIPAA provides many pathways for permissibly exchanging PHI. The fact sheets provide examples of actual scenarios to show how HIPAA supports the sharing of PHI for patient care, quality improvement, population health, and other activities.

The blog series discusses permitted uses and disclosures, and it gives examples of exchanges of health information for care coordination, care planning, and case management, both between providers and between provider and payers. The blog also provides examples of interoperable, permissible exchange of PHI for quality assurance and population-based activities. *(The blog is available at http://tinyurl.com/hhsfpkj. For more on misuse of HIPAA and what is allowed, see "Denying release of PHI can be a HIPAA violation,"* Healthcare Risk Management, *March 2016, at http://tinyurl.com/jdo9tb4.)* ■

Tenet to pay $238 million for false claims

Tenet Healthcare in Dallas has agreed to pay $238 million to resolve a False Claims Act lawsuit involving alleged kickbacks for maternity referrals by four of its hospitals.

The settlement is in response to a whistleblower lawsuit alleging fraud when the hospitals — Atlanta Medical Center; North Fulton Hospital, Roswell; Spalding Regional Hospital, Griffin; and Hilton Head Hospital on Hilton Head Island, SC — contracted with clinics operated by Hispanic Medical Management to provide prenatal care, predominantly to uninsured patients. The lawsuit claims that payments for translation, marketing, and help with Medicaid eligibility determinations actually were illegal kickbacks for referrals.

"We expect that the DOJ [Department of Justice] will make a counterproposal, and there can be no assurance that the ongoing discussions to resolve these matters will be successful," Tenet said in a recent filing to shareholders. "The terms of a final resolution may require us to pay significant fines and penalties and give rise to other costs or adverse consequences that materially exceed the reserve we have established." ■

TJC highlights project to reduce employee falls

The recent issue of the *International Journal of Six Sigma and Competitive Advantage* includes an article about the results of a project of The Joint Commission (TJC) that successfully reduced the average number of monthly falls of TJC field staff by 64.8% and has sustained the results for four years.

Solutions included emails to raise awareness of wearing the proper footwear and changing weather conditions, and a pamphlet about the risks associated with walking surface conditions, carrying work-related or personal items, and type of luggage used. The average monthly rate of falls was reduced by 64.8% during the post-intervention period.

An abstract is available online at http://tinyurl.com/zjppags. ■

Correction

In the April 2016 issue of *Healthcare Risk Management*, a story regarding accusations of sexual assault against a physician at Mount Sinai Hospital in New York City incorrectly referred to the physician as a surgeon. He was director of clinical research in emergency medicine at the time of the alleged incident but is no longer with the hospital. ■

Reader Survey has 2 options

This year, we offer you the option of taking the *2016 Reader Survey* in print, enclosed in this issue, or online, at http://svy.mk/1S1wIcT.

We look forward to receiving your feedback on how we can make *Healthcare Risk Management* as useful as possible. ■

CE/CME OBJECTIVES

Upon completion of this educational activity, participants should be able to:

1. describe the legal, clinical, financial, and managerial issues pertinent to risk management;
2. explain the impact of risk management issues on patients, physicians, nurses, legal counsel, and management;
3. identify solutions to risk management problems in healthcare for hospital personnel to use in overcoming the challenges they encounter in daily practice.

HEALTHCARE RISK MANAGEMENT™

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 the AHCMedia.com site to take a post-test. Go to "My Account" to view your available CE activities. First-time users will have to register on the site using the 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.

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

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

CE/CME QUESTIONS

1. **When Texas Children's Hospital in Houston assessed causes of alarm fatigue, how did the trash bins used on units contribute to excessive alarms?**

   A. Closing the lid made a loud noise that startled patients and triggered alarms because their heart rates went up.
   B. The metal bins amplified the sound of the alarms.
   C. Some device leads were activated when the wires touched the metal trash bins.
   D. There were not enough bins, so staff members were sometimes out of position and too far to respond promptly to an alarm.

2. **How did Texas Children's Hospital modify the threshold for SpO2 alarms?**

   A. The standard alarm threshold was changed from 93% to 90%, though physicians can set it differently for individual patients.
   B. The alarm threshold was changed from 93% to 90%, and physicians cannot modify it for any patient.
   C. The standard alarm threshold was changed from 90% to 93%, but only for surgical patients.
   D. The standard alarm threshold was changed from 90% to 93%, but only for intensive care patients.

3. **How much ransom did Hollywood Presbyterian Medical Center in Los Angeles pay in bitcoin to end a ransomware attack?**

   A. $10,000
   B. $17,000
   C. $87,000
   D. $2.3 million

4. **According to Amy Alderfer, JD, an attorney with the law firm of Cozen O'Connor in Los Angeles, what is one way a healthcare facility could face liability related to the recall of a duodenoscope manufactured by Olympus?**

   A. Strict liability for using the scope on the patient
   B. Failing to notify patients of an infection related to use of the scope
   C. Malpractice for using a defective instrument
   D. False Medicare claims for using a defective instrument

LEGAL REVIEW & COMMENTARY
EXPERT ANALYSIS OF RECENT LAWSUITS AND THEIR IMPACT ON HEALTHCARE RISK MANAGEMENT

Paperwork error leaves hospital without insurance and forced to defend malpractice suit on its own

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

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

David Vassalli, *2016 JD Candidate*
Pepperdine University School of Law
Malibu, CA

News: In 2008, a woman went to a hospital seeking treatment for weight and size reduction. A physician recommended a form of mesotherapy, which is a non-surgical technique to dissolve fat tissues through injections. Neither the treatment nor some of the drugs used in administering the therapy were approved by the Food and Drug Administration (FDA). Between 2008 and 2009, the mesotherapy and the injections involved with it were administered by a physician at a location other than the hospital. The woman allegedly developed painful and infected sores on her body from the mesotherapy and filed a malpractice action against the physician and the hospital that employed him. The woman alleged that the physician failed to inform her the treatment was experimental and not approved by the FDA and that the hospital that employed him was liable for his conduct. The woman's lawsuit requested $50,000 in compensation for her injuries. As is the case when hospitals and physicians are facing malpractice litigation, the hospital turned to its insurance company to defend the suit and provide coverage for the resulting liability. However, the insurance company refused to defend the hospital and asserted that the insurance forms contained misrepresentations that invalidated the insurance policy. The hospital argued that the policy used confusing language that the hospital did not technically violate by administering the mesotherapy injections away from the hospital. The insurance company then obtained a court order against the hospital declaring that the insurance policy was invalidated and that the physician's conduct was imputed to the hospital because that's where medical treatment began. The hospital is now without funded legal representation or liability coverage for the still-pending medical malpractice action for the woman's injuries caused by the mesotherapy injections.

Background: A woman visited a hospital seeking treatment for weight and size reduction in 2008. A physician at the hospital recommended mesotherapy, which aims to dissolve fatty tissues in the stomach. Mesotherapy involves a series of injections, and the treatment itself and drugs used are not approved by the FDA. From November 2008 to July 2009, the woman received the mesotherapy and injections from the physician at a location other than the hospital. At no point were the injections administered at the hospital. According to court documents, the woman developed "painful, infected, blister-like granulomas," which were similar to open sores, on her body. As a result of her injuries, the woman filed a malpractice lawsuit against the physician who recommended and administered the mesotherapy injections and the hospital that employed him. The woman particularly alleged that the physician failed to inform her the treatment was experimental and not approved by the FDA, that the hospital was liable for employing the physician, and that her injuries entitled her to $50,000 in

inancial Disclosure: Co-authors Jamie Terrence & David Vassalli, author Greg Freeman, Exec. Editor Joy Daughtery Dickinson, & Nurse Planner Maureen Archambault have no financial relationships with companies having ties to this field. Co-author Damian Capozzola represents Currie Medical Specialties in an action against Tenet Healthcare and is in an administrative action against Westside Regional Center. Arnold Mackles, physician reviewer, writes CME/CE courses, is on The Sullivan Group advisory group, & is a stockholder, speaker, author & consultant for Innovative Healthcare Compliance Group.

compensation.

The hospital did what nearly all businesses and professional service providers do when facing litigation for negligence, which is seek representation and shelter from direct financial liability from their insurance providers. However, the insurance company in this case refused to defend the hospital on the grounds that the insurance policy was invalid due to misrepresentations made by the hospital on the insurance forms. The initial paperwork asked whether the hospital's employees use drugs for weight reduction, if the practice includes weight reduction by methods other than diet or exercise, if the practice "dispenses drugs or injections" for weight control, and whether experimental procedures would be used. All of these questions on the form were answered in the negative. The hospital argued that the policy used confusing language regarding exactly what "use" of injections meant and the distinction between "weight reduction" and "size reduction," and that size reduction therapy performed outside of the hospital should not invalidate the contract.

The court agreed with the insurance company and ordered that the insurance policy is not valid because of the misrepresentations made by the hospital, and it said the insurance company is not required to represent the hospital or cover the financial liability arising from the incident. The court went on to say that the physician's behavior was imputed to the hospital because the events giving rise to the injections began at the hospital. The hospital appealed these decisions and lost the appeal on the same grounds. As a result of the paperwork being inaccurate and the outcomes of the surrounding litigation, the hospital must now fund its own legal representation and pay any damages that result from the woman's pending medical malpractice action.

What this means to you: This case demonstrates the utmost diligence with which insurance-related matters must be handled and how a few minor errors can leave hospitals and physicians without insurance when facing medical malpractice liability. All hospitals, medical centers, physicians, and healthcare providers should be fully aware of the exact terms of their insurance policies and make sure they are in compliance with their policies. If there is any uncertainty at any stage of the insurance process regarding exactly what conduct is covered by insurance or what the terms in the policy mean, an attorney should be consulted.

In this case, the hospital argued it did not fully understand the language in the insurance policy and that it believed it was acting in accordance with the policy, and therefore, the misrepresentations were unintentional and insignificant. However, the court rejected that argument and explained that because insurance policy terms and prices are guided by assessing the financial risk of covering a practice, any misrepresentation is significant and it does not matter that the mistake was unintentional. The strict approach taken to interpreting insurance policies in this manner is unfavorable to the practitioners in this case. The reality that a minor error in filling out the forms can leave a provider paying to defend against a lawsuit, and the award from that lawsuit, demonstrates the need to ensure physicians, hospitals, and all other providers operating under an insurance policy fully understand, update, and review their insurance policies to ensure they are in compliance at all times.

This case also illustrates the scope of activity that an employer can be held liable for regarding the conduct of its employee-physician. While states have varying approaches to the exact lines of when an employer is liable for the conduct of its employees, or even whether a physician can be a hospital employee at all, a common thread is that an employer is typically liable for the conduct of an employee, as opposed to a private contractor, when the employee's conduct giving rise to the lawsuit is inside the scope of employment.

Another common thread for holding an employer liable is when the employee acts in a manner that represents to the patient that the physician's actions are one and the same as the employer's. In this case, there was no dispute as to whether the physician who caused the alleged harm was an employee of the hospital, but rather the issue was whether the conduct that took place at a location other than the hospital was outside the scope of his employment or could be imputed to the hospital.

To establish that the conduct of the physician was imputed to the hospital in this case, the court pointed to the facts that the treatment first was recommended at the hospital, the physician never informed the patient he was working in any individual capacity, and the woman likely relied on the good reputation of the hospital in accepting treatment at a location other than the hospital. Accordingly, and despite the hospital arguing this conduct is not that of the hospital because it took place at a location other than the hospital, the hospital is liable for its employee's conduct and will have to defend against and pay

the damages of the ongoing lawsuit.

This precedent is controlling in the jurisdiction of the Seventh Circuit of the United States Court of Appeals, which includes Illinois, Indiana, and Michigan, and closely mirrors all other jurisdictions. The exact contours of when employees are acting inside the scope of their employment can vary depending on jurisdiction and should be known by healthcare employers in consultation with qualified counsel.

Nevertheless, this case demonstrates that an employer can be liable for its employee when the conduct begins in the healthcare facility, the patient is not informed that the physician is acting independently, and the patient relies on the reputation of the facility in accepting individual treatment from an employee. Bearing this in mind, healthcare facilities seeking to avoid liability for certain employee conduct should take steps to inform their patients of the relationships between the patient's physician and the healthcare facility, explain to employees that they must inform clients when they are no longer providing treatment backed by the healthcare facility, and retain all documents showing that the patient has been made aware the physician providing care is not an employee of the hospital or that certain conduct is outside the scope of employment. Employment agreements also might contain indemnification clauses through which the employee (and/or the employee's independent insurance) indemnifies the facility against any breaches.

REFERENCE

Case No. 14-1791 (Seventh Circuit. March 4, 2016) ■

Hospital is liable for $1.5 million for surgeon's failure to inspect surgery site

News: In 2011, a 51-year-old woman went to a hospital for a hysterectomy. An obstetrician who works at the hospital operated. The routine surgery went seemingly well, and the woman remained in the hospital for observation. On the fifth day of her postoperative stay, she developed a worsening infection in her abdomen. She was transferred to the Intensive Care Unit for her abdominal infection. The infection worsened over the following days. On the woman's 10th postop day at the hospital, she underwent surgery to address the infection. A different surgeon at the hospital performed the procedure to clean out the infection site. It was discovered during the procedure that the woman's intestines had been damaged by the infection. As a result of the damage the infection caused, the surgeon performed a colostomy. The woman used the colostomy bag for seven months and had to undergo two more surgeries to treat the infection. The woman filed a malpractice action against the obstetrician who performed the hysterectomy and the hospital that employed him. The woman alleged that the obstetrician, and the hospital as his employer, were negligent in failing to diagnose and treat lacerations to the bowel that occurred during the hysterectomy he performed, which caused the infection, damage to the intestines, and the need for more surgeries and the use of a colostomy bag. The obstetrician denied he committed negligence. During the trial, an expert surgeon called by the women's attorney testified that the standard of care when performing a hysterectomy is to inspect the surgery site for any lacerations made during the surgery and that the obstetrician failed to do so here. With this in mind, the jury sided with the woman and ordered that the hospital pay her an award of $1.5 million. The award consisted of $800,000 for future pain and suffering, $700,000 for past pain and suffering, and $20,000 in lost wages.

Background: A woman went to the hospital for a hysterectomy. The surgery was performed in April 2011 by an obstetrician at the hospital. There were no known complications during the surgery, and the woman was to remain in the hospital while she recovered. However, experts and medical records at trial later showed that the women's bowel, located above the uterus that was removed during her hysterectomy, was cut. Five days after the surgery and while still at the hospital, the woman developed a worsening infection in her abdominal area. She was transferred to the Intensive Care Unit, and the infection continued to worsen in the following days.

Ten days after the hysterectomy, the woman's abdominal infection became severe, and another surgery was ordered to clean it out. A different surgeon than the one who performed the hysterectomy performed the procedure, which took place at the same hospital. During the procedure, the surgeon discovered that the woman's intestines

had been damaged by the infection. This damage required the surgeon to perform a colostomy so that the woman's waste would not pass through the infected area. Two more surgeries were required to treat her infection.

The woman filed a malpractice lawsuit against the obstetrician who performed the hysterectomy. The hospital also was named as a defendant because the hospital employed the obstetrician. The woman alleged that the obstetrician negligently failed to diagnose and treat lacerations in her bowel that occurred during the hysterectomy he performed and that these lacerations caused the infection, the subsequent damage to her intestines, and the need to undergo two more surgeries to treat the infection as well as the need for a colostomy bag for seven months after the surgery. The woman's attorney called expert surgeons to testify during the trial, and the experts testified that the obstetrician had a duty to carefully inspect the surgery site for any lacerations. It was further declared that the obstetrician failed to perform this inspection before closing the surgery site, which caused the infection and led to the subsequent damages the woman suffered. The jury found in favor of the woman and held the hospital liable for the $1.5 million verdict, which consisted of $800,000 for future pain and suffering, $700,000 for past pain and suffering, and $20,000 in lost wages.

What this means to you: This case is an example of an expert establishing the standard of care that physicians are expected to follow during their practice of medicine. The attorney of the former patient will commonly use experts to explain the standard of care that the physician has a duty to follow, and then the jury determines whether the physician breached that duty and how much damage that breach caused. Prudent healthcare practitioners should be aware of the standards they are expected to follow when administering care. The damage in this case came from a bowel injury, which is a relatively common source of medical malpractice litigation. Experts at trial testified that the standard that is to be followed when performing a hysterectomy is to closely examine the bowel and surrounding area before closing the operative site. Additional standards that have been recognized for operating near the bowel call for an examination of the bowel to ensure it has not been lacerated, perforated, or otherwise affected by a nearby surgery. If the bowel has been damaged, infection is a common symptom, and physicians should monitor the patient for signs of infection. As this case shows, there are acceptable standards of care with which physicians have a legal duty to comply, and failure to do so can lead to liability. Practitioners need to be aware of the standards guiding their areas of practice and should take steps that demonstrate and document that the practitioners complied with that standard when administering healthcare. For example, when a surgeon dictates the operative report, he or she should use this opportunity to describe how actions taken meet the standard of care. Describing an inspection of the operative area, even if no adverse finding is seen, may protect the practitioner from future liability, even if something is missed. Due diligence, when documented, combined with documented informed consent of the common risks such as a perforation or laceration of a nearby organ, can mitigate damages.

This case also illustrates how the postoperative care a patient receives can lead to liability. While it was negligent not to closely investigate the woman's bowel when operating near it, the damages the woman suffered occurred in the following 10 days. It should be noted that medical malpractice jury awards are based on (and should be limited to) the damages the patient suffered by the harm that was negligently caused. As such, mitigating the harm a patient suffers following a negligent act is an important way to reduce the amount of financial liability a physician or a hospital ultimately will face. In this case, the damage the woman suffered was primarily caused by the infection that hospital staff did not clean out until five days after learning the woman was suffering from an infection in the area on which other hospital staff recently had operated. Had the woman's infection been adequately addressed earlier, the damages she suffered would have been further mitigated, and the hospital would have incurred less financial liability for the incident.

Similarly, had the infection gone wholly untreated, the damages suffered by the patient likely would have been significantly greater. As is illustrated by the financial liability the hospital faces being directly related to the damages a patient suffers, addressing complications and health concerns of patients who already have received care at the healthcare facility in an expedient and effective manner can greatly reduce the amount of financial liability the healthcare facility will face for a past act of negligence.

REFERENCE

Schenectady County Supreme Court, New York. Case No 2013-762 (March 2, 2016). ■

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

Don't forget that small HIPAA violations can cause big problems for hospitals

The large data breaches that compromise the protected health information (PHI) of thousands of people are the ones that receive all the attention, but the smaller violations of the Health Insurance Portability and Accountability Act (HIPAA) can be just as harmful, if not more so, to those involved. Healthcare leaders too often devote most of their attention to the large breaches and not enough to the more common, smaller violations, experts say.

A breach involving 500 to 10,000 patients generally is considered small in the healthcare community. The ramifications of a large data breach are well known, notes **Deborah Gersh**, JD, an attorney with the Chicago law firm of Ropes & Gray, but a breach involving only 500 patients still can be serious for the hospital or health system. The Health and Human Services (HHS) Office for Civil Rights (OCR) uses 500 affected individuals as the cutoff for reporting HIPAA breaches; a breach of 500 or more must be reported immediately, but smaller breaches can be reported annually. Once a breach of 500 or more is reported and posted on the OCR web site, the information is available to anyone.

"There are people who troll the site looking for breaches that have the potential for class action on the state level," Gersh warns. "And the report of 500 or more triggers an automatic inquiry by OCR. That can be a fairly robust response that will be a significant event for the healthcare provider."

In addition, OCR will want to see the healthcare entity's HIPAA risk analysis. Even if the analysis was conducted under privilege, OCR takes the position that it can access the document because the analysis is a required document for HIPAA compliance, Gersh says. OCR will retain a copy of the analysis in its records, which are subject to Freedom of Information Act requests and other public access.

"Sometimes that analysis is very honest in describing the things that could be improved, particularly when the company gets a third party to conduct the analysis and make it as objective as possible," Gersh says. "That can place the company in a very vulnerable position if that information is disclosed and someone wants to use it against the hospital in litigation."

> "IT'S DEATH BY A THOUSAND CUTS. IF YOU DON'T HAVE A CULTURE THAT TAKES THESE SMALLER VIOLATIONS SERIOUSLY, THEY ADD UP ..."

Action plan can be costly

A small breach can lead to a corrective action plan, just as with larger breaches, and that plan can create significant costs for the healthcare entity, Gersh says.

The plan may call for updating security and data management systems, improvements that can be a financial challenge for smaller hospitals or systems, she says. They already are squeezed by the cost of system updates that used to come every few years but now are sometimes needed on a monthly basis, and adding improvements from a corrective action plan can make their data management costs rise even more. *(A noteworthy civil monetary penalty from OCR involved fewer than 500 records. See the story in this issue.)*

"I see a lot of smaller hospitals and doctors' offices

struggle with that," Gersh says. "A corrective action plan commonly calls for more training for staff, and that carries a price both in terms of paying someone for the training and also in terms of staff time away from their jobs. These costs add up, and a corrective action plan can force you to make improvements and updates that you had not budgeted for yet."

The smaller violations involving 500 or fewer patients are less likely to be the result of a deliberate intrusion by hackers, who typically can access many thousands of records once they gain access. They are more likely to occur from carelessness by employees who leave a laptop in a public place, for example, Gersh says. That likelihood of occurrence means that hospital administrators must not lose focus on educating employees about physical data security while focusing on the complexities of digital security, she says.

Administrators should seek opportunities to reinforce the need for physical security of documents and hardware, Gersh suggests. Some facilities have a HIPAA security huddle with staff at regular intervals, in which employees and administrators can discuss any questions and note possible security risks, she notes. Others send casual "Did you know…" reminders by email to reinforce good security practices. In either format, the administrator might point out that patient charts were left unattended at a nurses' station, for example, or that a jump drive was left at a computer station.

"The anecdotal reports have a big impact on staff," Gersh says. "The employees can see how all the talk about HIPAA security manifests itself in their daily routines."

Instilling the right culture may require educating the top brass, in addition to the front-line employees who handle PHI. The culture of a healthcare institution must emphasize that smaller HIPAA violations are as important as the larger ones, and the culture emanates from the C-suite, says **Susan Tellem**, RN, BSN, APR, a partner with Tellem Grody Public Relations, in Los Angeles, which assists providers with the response to HIPAA violations.

"It's death by a thousand cuts. If you don't have a culture that takes these smaller violations seriously, they add up, and it becomes a bigger problem," Tellem says. "This is a top down issue, and the board of directors often doesn't even understand HIPAA. The CEO and the board of directors need to understand that it's not just the big fish that they should worry about, that the culture has to instill a respect for HIPAA security on an individual level."

Personal impact

The impact on the individual whose data is compromised can be significant whether that one person comprises the entire breach or whether the person is one of thousands, Tellem notes. When private information is released, there is the possibility that someone will use that data in a way that harms the person financially or in a personal way, and the healthcare entity that failed to protect it will be held responsible.

A large breach immediately brings the likelihood of fines from OCR, the associated costs of a corrective action plan, and bad publicity for the institution. But with a smaller breach, there is still the potential for major liability, Tellem notes.

"If someone loses a job or a patient is revealed to have HIV or mental health problems, something not always looked kindly upon by the general population, that becomes a liability for the institution, which can face huge lawsuits," Tellem says. "Those lawsuits will generate publicity, which also harms the hospital's reputation. All of that can come from failing to protect just one patient's protected health information."

One area of particular risk is when a healthcare entity wants to tell a patient's story or use before-and-after photos, Tellem notes. Although highly desired for marketing purposes, the healthcare provider must be certain that the patient has provided written permission for the use of the story or photos in all intended formats. Don't overlook getting permission for the material to be used in social media, she advises.

Tellem agrees with Gersh that ongoing staff education is key to preventing smaller HIPAA breaches, with anecdotes about how privacy can be compromised inadvertently.

"Use breaches at other institutions as an example so that it doesn't happen at yours. If you just say 'be careful with patient data,' that doesn't mean much," Tellem says. "But if you talk about how a nurse somewhere else took a selfie that happened to show patient data in the background, they can relate to that. Front-line employees might not think they have much to do with preventing a loss of 50,000 records, but you can remind them that they have a lot of control over the security of each individual record they handle."

SOURCES

- **Deborah Gersh,** JD, Ropes & Gray, Chicago. Email: Deborah.gersh@ropesgray.com.
- **Susan Tellem**, RN, BSN, APR, Partner, Tellem Grody, Los Angeles. Telephone: (310) 313-3444. Email: susan@tellemgrodypr.com. ■

Decision on Lincare civil penalties should be a reminder of liability potential

The latest development in a Health Insurance Portability and Accountability Act (HIPAA) breach investigation should serve as a reminder that fines are not the only way the government can punish a healthcare institution for failing to protect patient information. Civil penalties are possible, and the courts are upholding their legality.

In addition, the case is demonstrating that inquiries by the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) should be taken seriously from the outset.

An HHS administrative law judge (ALJ) recently ruled that Lincare, a provider of respiratory care, infusion therapy, and medical equipment to in-home patients, with more than 850 branch locations in 48 states, violated HIPAA and granted summary judgment to the OCR on all issues. The ruling requires Lincare to pay $239,800 in civil monetary penalties imposed by OCR. This is only the second time in its history that OCR has sought civil monetary penalties for HIPAA violations, and each time the penalties have been upheld by the ALJ.

OCR's investigation of Lincare began after an individual complained that a Lincare employee left behind documents containing the protected health information (PHI) of 278 patients after moving residences. Evidence established that this employee removed patients' information from the company's office, left the information exposed in places where an unauthorized person had access, and then abandoned the information altogether, according to OCR.

During the investigation, OCR found that Lincare had inadequate policies and procedures to safeguard patient information that was taken offsite, although employees, who provide healthcare services in patients' homes, regularly removed material from the business premises. Further evidence indicated that the organization had an unwritten policy requiring certain employees to store PHI in their own vehicles for extended periods of time, according to the OCR report. Although aware of the complaint and OCR's investigation, Lincare subsequently took only minimal action to correct its policies and strengthen safeguards to ensure compliance with the HIPAA rules, OCR told the court.

"While OCR prefers to resolve issues through voluntary compliance, this case shows that we will take the steps necessary, including litigation, to obtain adequate remedies for violations of the HIPAA Rules," OCR Director **Jocelyn Samuels** said in a statement released after the ALJ decision. "The decision in this case validates the findings of our investigation. Under the ALJ's ruling, all covered entities, including home health providers, must ensure that, if their workforce members take protected health information offsite, they have adequate policies and procedures that provide for the reasonable and appropriate safeguarding of that PHI, whether in paper or electronic form."

Lincare claimed that it had not violated HIPAA because the PHI was "stolen" by the individual who discovered it on the premises previously shared with the Lincare employee. The ALJ rejected this argument and said Lincare was obligated to take reasonable steps to protect its PHI from theft. *(The Notice of Proposed Determination and the ALJ's opinion may be found on the HHS website at http://1.usa.gov/1P6APVD.)* The company could appeal to one more level but has not indicated it will do so.

Off-site employees

The case holds important lessons for any company that needs employees to work remotely with PHI, notes **Christine G. Savage**, JD, an attorney with the law firm of Choate Hall and Stewart in Boston. The employers should conduct or update a risk analysis to determine the biggest risks for HIPAA violations with these off-site employees, and they should instill appropriate policies and procedures, she says.

"Lincare did not have any policies and procedures in 2008, and at least the first half of 2009, that addressed how people were to safeguard information when they took it off site," Savage explains. "There were no policies about how to check data in and out, or to record how long you had possession of the information. There was no policy on the appropriate storage of that material if you couldn't get it back to the office at the end of the day."

The Lincare case also indicates that OCR is concerned not only with the number of people affected by a breach, but also the nature of the breach, Savage notes. OCR determined that 278 patients' PHI was compromised.

Most of the civil monetary penalty relates to the lack of policies and OCR's claim that Lincare did

nothing to enact policies even after the deficit was brought to company's attention. Savage says this penalty is a reminder to take seriously any concerns of this type coming from the government. If OCR says your policies are inadequate or you haven't conducted a risk analysis, and you don't do anything in response, regulators are likely to look on the violations as more serious and look to civil monetary penalties to get your attention, she says. A slow or less-than-enthusiastic response may end with the same result.

Evidence cited in the ALJ decision suggests that the Lincare chief compliance officer was flippant in responding to OCR. The compliance officer replied to OCR by saying something to the effect of "we thought about putting in place a policy that you shouldn't let anybody steal your stuff," but found it unnecessary. OCR offered to settle the case, but Lincare refused a voluntary resolution, which typically involves a corrective action plan including a period of monitoring.

"Some of it may have been an attitudinal issue with regard to this particular company, which obviously isn't helpful," Savage says. "They may have made a calculated decision that OCR wouldn't pursue it to this level."

Lincare's position was that it was the victim in this case because the patient records were stolen, notes **Roy Wyman**, JD, partner with the law firm of Nelson Mullins in Nashville, TN. That position may explain some of the company's response, or lack of response, to the OCR inquiry, Wyman says.

One lesson from the case is that in addition to protecting PHI and having proper policies and procedures, you also must be prepared to demonstrate that you care about privacy if OCR ever comes calling, he says. Whether you think the breach was your fault or not, start out by conveying that you take seriously any suggestion that your HIPAA compliance program may be inadequate.

You still can make the argument later that OCR is misinterpreting the circumstances or try to prove that your policies and procedures were sufficient, but Wyman says the Lincare experience demonstrates that you must start off on the right foot with OCR. Wyman notes that OCR's arguments before the ALJ suggest that it was not going to come down too hard on the fact that employees were driving around with physical records, and that it was willing to acknowledge that securing those documents was difficult.

"In the end, the message is that you can't be combative and respond with a litigious attitude right from the start," Wyman says. "They could have settled and probably should have. Sometimes you need to take your lumps and accept it. That seems to be where Lincare had a problem, saying they weren't at fault and willing to take it to the limit."

Savage points out that the person who found the PHI was the Lincare employee's husband. The couple was splitting up, and after the employee left the home, her husband found the patient information and reported it. One explanation for Lincare's apparently inadequate response could be that the company leaders thought they were being drawn into an employee's divorce and personal life, with the husband reporting the find to cause trouble for his wife and the company.

"They may have thought this was much ado about nothing and found several years later that OCR took it seriously," Savage says. "I would never advise that if OCR expresses concern about your policy, that you leave that policy alone. You should be asking what you need to do to tweak it, or have a discussion with OCR about why you think you don't need to." ■

OCR: Facilities need organization-wide risk analysis

The University of Washington Medicine (UWM) in Seattle has agreed to settle charges that it potentially violated the Health Insurance Portability and Accountability Act (HIPAA) by failing to implement policies and procedures to prevent, detect, contain, and correct security violations. The Department of Health and Human Services Office for Civil Rights (OCR) reports that the settlement should underscore the necessity of conducting organization-wide risk analysis.

The settlement includes a monetary payment of $750,000, a corrective action plan, and annual reports on the organization's compliance efforts.

OCR initiated its investigation of UWM following receipt of a breach report on Nov. 27, 2013, which indicated that the electronic protected health information (PHI) of approximately 90,000 individuals was accessed after an employee downloaded an email attachment that contained malicious malware. TOCR's investigation indicated UWM's security policies required its affiliated entities to have up-to-date, documented system-level risk assessments and to implement safeguards in compliance with the Security Rule. ■

Healthcare Risk Management

2016 Reader Survey

In an effort to learn more about the professionals who read *HRM,* we are conducting this reader survey. The results will be used to enhance the content and format of *HRM.* Instructions: Fill in the appropriate answers. Please write in answers to the open-ended questions in the space provided. **Please fax the completed questionnaire to 678-974-5419, return it in the enclosed postage-paid envelope, or complete it online at https://www.surveymonkey.com/r/HRMAnnualReaderSurvey2016.**

1. Please fill in all the areas for which you are responsible for risk management in your facility or system.

- O A. acute care
- O B. outpatient services
- O C. same-day surgery
- O D. home health services
- O E. rehabilitation services
- O F. extended care facility
- O G. hospice

In future issues of *HRM,* would you like to see more or less coverage of the following topics?

	A. more coverage	B. less coverage	C. about the same amount
2. compliance	O A	O B	O C
3. malpractice	O A	O B	O C
4. patient safety	O A	O B	O C
5. patient restraints	O A	O B	O C
6. informed consent	O A	O B	O C
7. patient confidentiality/privacy	O A	O B	O C
8. patient falls	O A	O B	O C
9. medical errors	O A	O B	O C
10. root-cause analysis	O A	O B	O C
11. sentinel event reporting	O A	O B	O C
12. accreditation issues/audits	O A	O B	O C

13. Do you find the *Legal Review & Commentary* insert in *HRM* helpful?

O A. yes O B. no

14. Including *HRM*, which publication or information source do you find most useful, and why?

_____

_____

15. Do you plan to renew your subscription to *HRM*?

- O A. yes
- O B. no If no, why not?_____

_____

16. Are the articles in *HRM* written about issues of importance and concern to you?

- O A. always
- O B. most of the time
- O C. some of the time
- O D. rarely
- O E. never

17. How would you describe your satisfaction with your subscription to *Healthcare Risk Management* newsletter?

- O A. very satisfied
- O B. somewhat satisfied
- O C. somewhat dissatisfied
- O D. very dissatisfied

18. Which best describes your title?

- O A. risk manager or risk management director
- O B. VP or assistant administrator
- O C. director/manager of quality
- O D. medical director or director of nursing
- O E. other_____

19. Please indicate all of the activities for which you have primary management responsibility.

- O A. risk management
- O B. compliance
- O C. legal
- O D. quality or utilization review
- O E. other_____

20. Which area at your facility triggered the most incident reports in 2014?

- O A. emergency department
- O B. medical
- O C. obstetrics
- O D. operating room
- O E. other _____

Please rate your level of satisfaction with the following items.
A. excellent B. good C. fair D. poor

21. Quality of newsletter	○ A	○ B	○ C	○ D
22. Article selections	○ A	○ B	○ C	○ D
23. Timeliness	○ A	○ B	○ C	○ D
24. Length of newsletter	○ A	○ B	○ C	○ D
25. Overall value	○ A	○ B	○ C	○ D
26. Customer service	○ A	○ B	○ C	○ D

27. On average, how many people read your copy of *HRM*?

○ A. 1
○ B. 2
○ C. 3
○ D. 4
○ E. 5 or more

28. What is the bed size of your facility/system?

○ A. fewer than 200 beds
○ B. 200 to 400 beds
○ C. 401 to 600 beds
○ D. 601 to 800 beds
○ E. more than 800 beds

29. On average, how many articles in *HRM* do you find useful?

○ A. none
○ B. 1-2
○ C. 3-4
○ D. 5-6
○ E. 7 or more

30. What do you like most about *HRM* newsletter?

31. What do you like least about *HRM* newsletter?

32. Please list the top three challenges you face in your job today.

33. What issues would you like to see addressed in *HRM* newsletter?

Contact information